Table of Contents

Welcome to Tenable.io ................................................................. 31

Get Started with Vulnerability Management ................................... 33

Get Started with Lumin ............................................................... 39

Get Started with WAS ............................................................... 43

Get Started with CS ................................................................. 47

System Requirements .................................................................. 48

WAS Requirements .................................................................... 49

CS Requirements ....................................................................... 50

Vulnerability Management Licenses .............................................. 52

WAS Licenses ............................................................................ 56

Log in to Tenable.io ..................................................................... 58

Navigate Tenable.io (New Interface) ............................................ 59

Transition to the New Interface .................................................. 60

Transition to the New WAS Interface ......................................... 67

Activate the New Interface for WAS ......................................... 71

Interface Activation Modes in WAS .......................................... 72

Access the New Interface ........................................................ 73

View Notifications ..................................................................... 74

Access the User Account Menu ................................................ 75

Access the Quick Actions Menu ............................................... 76

Access the Resource Center ..................................................... 77

Navigate Breadcrumbs ................................................................ 78
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate Planes</td>
<td>79</td>
</tr>
<tr>
<td>Tenable.io Tables</td>
<td>80</td>
</tr>
<tr>
<td>Interact with a Standard Table</td>
<td>81</td>
</tr>
<tr>
<td>Interact with a Customizable Table</td>
<td>83</td>
</tr>
<tr>
<td>Filter a Table</td>
<td>86</td>
</tr>
<tr>
<td>Clear Table Filters</td>
<td>89</td>
</tr>
<tr>
<td>Saved Search</td>
<td>90</td>
</tr>
<tr>
<td>Create a Saved Search</td>
<td>91</td>
</tr>
<tr>
<td>Edit a Saved Search</td>
<td>92</td>
</tr>
<tr>
<td>Apply a Saved Search</td>
<td>94</td>
</tr>
<tr>
<td>Share a Saved Search</td>
<td>95</td>
</tr>
<tr>
<td>Delete a Saved Search</td>
<td>96</td>
</tr>
<tr>
<td>Return to the Classic Interface</td>
<td>97</td>
</tr>
<tr>
<td>Log Out of the New Interface</td>
<td>98</td>
</tr>
<tr>
<td>Navigate Tenable.io (Classic Interface)</td>
<td>99</td>
</tr>
<tr>
<td>Search (Classic Interface)</td>
<td>100</td>
</tr>
<tr>
<td>Navigate the Classic Interface in WAS (Classic Interface)</td>
<td>101</td>
</tr>
<tr>
<td>Scans</td>
<td>104</td>
</tr>
<tr>
<td>Vulnerability Management Scanning Overview</td>
<td>106</td>
</tr>
<tr>
<td>Discovery Scans vs. Assessment Scans</td>
<td>108</td>
</tr>
<tr>
<td>Example: Identify Assets That Have Not Been Assessed</td>
<td>110</td>
</tr>
<tr>
<td>Example: Tag-Based Scanning</td>
<td>112</td>
</tr>
<tr>
<td>Example: Scan Routing</td>
<td>115</td>
</tr>
<tr>
<td>Scan Status</td>
<td>119</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Download the Tenable.io CS Scanner</td>
<td>167</td>
</tr>
<tr>
<td>Tenable.io CS Scanner Environment Variables</td>
<td>169</td>
</tr>
<tr>
<td>Configure and Run the Tenable.io CS Scanner</td>
<td>183</td>
</tr>
<tr>
<td>Scan an Image via the Tenable.io CS Scanner</td>
<td>184</td>
</tr>
<tr>
<td>Scan a Registry via the Tenable.io CS Scanner</td>
<td>186</td>
</tr>
<tr>
<td>Prepare your Registry</td>
<td>188</td>
</tr>
<tr>
<td>Glossary of CS Terms</td>
<td>191</td>
</tr>
<tr>
<td>PCI ASV Scanning Overview</td>
<td>193</td>
</tr>
<tr>
<td>Submit a Scan to the PCI ASV Dashboard</td>
<td>195</td>
</tr>
<tr>
<td>Create an Attestation</td>
<td>196</td>
</tr>
<tr>
<td>Mark an Asset as Out of Scope</td>
<td>198</td>
</tr>
<tr>
<td>Disputes</td>
<td>200</td>
</tr>
<tr>
<td>Create a Dispute</td>
<td>201</td>
</tr>
<tr>
<td>Edit a Dispute</td>
<td>204</td>
</tr>
<tr>
<td>Clone a Dispute to an Attestation</td>
<td>205</td>
</tr>
<tr>
<td>Delete a Dispute</td>
<td>207</td>
</tr>
<tr>
<td>Dispute Reasons</td>
<td>209</td>
</tr>
<tr>
<td>Submit an Attestation for ASV Review</td>
<td>211</td>
</tr>
<tr>
<td>Respond to an ASV Review Information Request</td>
<td>214</td>
</tr>
<tr>
<td>PCI ASV Scans (Classic Interface)</td>
<td>216</td>
</tr>
<tr>
<td>Submit a Scan to the PCI ASV Workbench (Classic Interface)</td>
<td>218</td>
</tr>
<tr>
<td>Create an Attestation (Classic Interface)</td>
<td>220</td>
</tr>
<tr>
<td>Mark an Asset as Out of Scope (Classic Interface)</td>
<td>222</td>
</tr>
<tr>
<td>Disputes (Classic Interface)</td>
<td>223</td>
</tr>
<tr>
<td>Function</td>
<td>Page</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Create a Dispute (Classic Interface)</td>
<td>224</td>
</tr>
<tr>
<td>Edit a Dispute (Classic Interface)</td>
<td>227</td>
</tr>
<tr>
<td>Clone a Dispute to an Attestation (Classic Interface)</td>
<td>228</td>
</tr>
<tr>
<td>Delete a Dispute (Classic Interface)</td>
<td>230</td>
</tr>
<tr>
<td>Submit an Attestation for ASV Review (Classic Interface)</td>
<td>231</td>
</tr>
<tr>
<td>Respond to an ASV Review Information Request (Classic Interface)</td>
<td>234</td>
</tr>
<tr>
<td>Manage Scans</td>
<td>236</td>
</tr>
<tr>
<td>Create a Vulnerability Management Scan</td>
<td>237</td>
</tr>
<tr>
<td>Edit a Vulnerability Management Scan Configuration</td>
<td>240</td>
</tr>
<tr>
<td>Create a WAS Scan</td>
<td>243</td>
</tr>
<tr>
<td>Edit WAS Scan Settings</td>
<td>246</td>
</tr>
<tr>
<td>Set WAS Scan Permissions</td>
<td>248</td>
</tr>
<tr>
<td>Copy a Scan Configuration</td>
<td>251</td>
</tr>
<tr>
<td>Change Scan Ownership</td>
<td>253</td>
</tr>
<tr>
<td>Organize Scans by Folder</td>
<td>255</td>
</tr>
<tr>
<td>Create a Custom Scan Folder</td>
<td>257</td>
</tr>
<tr>
<td>Move a Scan to a Scan Folder</td>
<td>258</td>
</tr>
<tr>
<td>Rename a Custom Scan Folder</td>
<td>260</td>
</tr>
<tr>
<td>Delete a Custom Scan Folder</td>
<td>262</td>
</tr>
<tr>
<td>Move a Scan to the Trash Folder</td>
<td>263</td>
</tr>
<tr>
<td>Delete a Scan</td>
<td>265</td>
</tr>
<tr>
<td>Delete a Remediation Scan</td>
<td>267</td>
</tr>
<tr>
<td>View Scans</td>
<td>269</td>
</tr>
<tr>
<td>WAS Scan Filters</td>
<td>273</td>
</tr>
</tbody>
</table>
View Vulnerability Management Scan Details .................................................. 274
View WAS Scan Details .................................................................................. 282
  Scan Notes Severity Details in WAS .......................................................... 287
Launch a Vulnerability Management Scan ..................................................... 289
Launch a Remediation Scan .......................................................................... 291
Launch a WAS Scan ......................................................................................... 299
  View WAS Scan Progress ...................................................................... 301
Pause or Resume a Scan .................................................................................. 302
Stop a Running Scan ...................................................................................... 303
Import a Scan .................................................................................................. 305
Delete a Scan Job ............................................................................................ 307
Change the Scan Read Status ......................................................................... 309
Unarchive a Scan ............................................................................................ 310
Export Scan Results ........................................................................................ 311
Scan Templates and Settings .......................................................................... 315
  Scan Templates .............................................................................................. 316
    Tenable-Provided Scanner Templates ....................................................... 317
    Tenable-Provided Agent Templates .......................................................... 320
    Tenable-Provided WAS Templates ............................................................. 321
    User-Defined Templates .......................................................................... 324
      Create a User-Defined Template ............................................................. 325
      Edit a User-Defined Template ................................................................. 328
      Copy a User-Defined Template .............................................................. 331
      Export a User-Defined Template ............................................................ 332
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import a User-Defined Template</td>
<td>333</td>
</tr>
<tr>
<td>Change User-Defined Template Ownership</td>
<td>334</td>
</tr>
<tr>
<td>Delete a User-Defined Template</td>
<td>336</td>
</tr>
<tr>
<td>Scan Settings</td>
<td>338</td>
</tr>
<tr>
<td>Basic Settings in Vulnerability Management Scans</td>
<td>340</td>
</tr>
<tr>
<td>Scan Targets</td>
<td>347</td>
</tr>
<tr>
<td>Basic Settings in WAS Scans</td>
<td>350</td>
</tr>
<tr>
<td>Basic Settings in User-Defined Templates</td>
<td>354</td>
</tr>
<tr>
<td>Discovery Settings in Vulnerability Management Scans</td>
<td>361</td>
</tr>
<tr>
<td>Preconfigured Discovery Settings</td>
<td>370</td>
</tr>
<tr>
<td>Scope Settings in WAS Scans</td>
<td>386</td>
</tr>
<tr>
<td>Assessment Settings in Vulnerability Management Scans</td>
<td>390</td>
</tr>
<tr>
<td>Preconfigured Assessment Settings</td>
<td>405</td>
</tr>
<tr>
<td>Assessment Settings in WAS Scans</td>
<td>413</td>
</tr>
<tr>
<td>Report Settings in Vulnerability Management Scans</td>
<td>417</td>
</tr>
<tr>
<td>Report Settings in WAS Scans</td>
<td>419</td>
</tr>
<tr>
<td>Advanced Settings in Vulnerability Management Scans</td>
<td>420</td>
</tr>
<tr>
<td>Preconfigured Advanced Settings</td>
<td>426</td>
</tr>
<tr>
<td>Advanced Settings in WAS Scans</td>
<td>435</td>
</tr>
<tr>
<td>Credentials in Vulnerability Management Scans</td>
<td>440</td>
</tr>
<tr>
<td>Add a Credential to a Scan</td>
<td>443</td>
</tr>
<tr>
<td>Edit a Credential in a Scan</td>
<td>446</td>
</tr>
<tr>
<td>Convert a Scan-specific Credential to a Managed Credential</td>
<td>447</td>
</tr>
<tr>
<td>Add a Credential to a User-defined Template</td>
<td>449</td>
</tr>
</tbody>
</table>
Edit a Credential in a User-defined Template .................................................. 451
Cloud Services ................................................................................................. 452
Database Credentials ...................................................................................... 456
  Database Credentials Authentication Types .................................................. 462
Host .................................................................................................................. 476
Privilege Escalation ......................................................................................... 505
Miscellaneous ................................................................................................. 509
Mobile ................................................................................................................ 513
Patch Management ............................................................................................ 518
Plaintext Authentication ................................................................................... 529
Credentials in WAS Scans ................................................................................ 535
  Configure Credentials Settings in a WAS Scan ............................................... 537
  Configure Selenium Credentials Settings Automatically .................................. 539
    WAS Selenium Commands ............................................................................. 542
HTTP Server Authentication Settings in WAS Scans ........................................ 546
WAS Scan Web Application Authentication .................................................... 547
Compliance in Vulnerability Management Scans ............................................ 550
SCAP Settings in Vulnerability Management Scans ....................................... 553
Configure Plugins in Vulnerability Management Scans ................................. 555
  Plugins (Classic Interface) .............................................................................. 558
    Plugin Settings in WAS Scans ....................................................................... 559
Target Groups .................................................................................................... 562
  Create a Target Group .................................................................................... 563
  Configure User Permissions for a Target Group ............................................. 565
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit a Target Group</td>
<td>567</td>
</tr>
<tr>
<td>Import a Target Group</td>
<td>569</td>
</tr>
<tr>
<td>Export a Target Group</td>
<td>571</td>
</tr>
<tr>
<td>Delete a Target Group</td>
<td>573</td>
</tr>
<tr>
<td>Target Group Permissions</td>
<td>575</td>
</tr>
<tr>
<td>Target Groups (Classic Interface)</td>
<td>576</td>
</tr>
<tr>
<td>Create a Target Group (Classic Interface)</td>
<td>577</td>
</tr>
<tr>
<td>Configure Permissions for a Target Group (Classic Interface)</td>
<td>579</td>
</tr>
<tr>
<td>Edit a Target Group (Classic Interface)</td>
<td>581</td>
</tr>
<tr>
<td>Import a Target Group (Classic Interface)</td>
<td>583</td>
</tr>
<tr>
<td>Export a Target Group (Classic Interface)</td>
<td>585</td>
</tr>
<tr>
<td>Delete a Target Group (Classic Interface)</td>
<td>587</td>
</tr>
<tr>
<td>Exclusions</td>
<td>589</td>
</tr>
<tr>
<td>Create an Exclusion</td>
<td>590</td>
</tr>
<tr>
<td>Edit an Exclusion</td>
<td>591</td>
</tr>
<tr>
<td>Import an Exclusion</td>
<td>592</td>
</tr>
<tr>
<td>Exclusion Import File</td>
<td>593</td>
</tr>
<tr>
<td>Export an Exclusion</td>
<td>595</td>
</tr>
<tr>
<td>Delete an Exclusion</td>
<td>597</td>
</tr>
<tr>
<td>Exclusion Settings</td>
<td>598</td>
</tr>
<tr>
<td>Exclusions (Classic Interface)</td>
<td>599</td>
</tr>
<tr>
<td>Create an Exclusion (Classic Interface)</td>
<td>601</td>
</tr>
<tr>
<td>Edit an Exclusion (Classic Interface)</td>
<td>602</td>
</tr>
<tr>
<td>Import an Exclusion (Classic Interface)</td>
<td>603</td>
</tr>
</tbody>
</table>
Export an Exclusion (Classic Interface) ................................................................. 604
Delete an Exclusion (Classic Interface) ................................................................. 606
Scans (Classic Interface) .......................................................................................... 607
Scanning Overview (Classic Interface) ..................................................................... 608
Scan Status (Classic Interface) ................................................................................. 610
Create and Manage Scans (Classic Interface) ......................................................... 611
Create a Scan (Classic Interface) ............................................................................. 612
Create a Limited Plugin WAS Scan (Classic Interface) ........................................... 614
WAS Chrome Extension (Classic Interface) ............................................................. 618
Create an Agent Scan (Classic Interface) ................................................................. 629
Import a Scan (Classic Interface) ............................................................................. 630
Launch a Scan (Classic Interface) ........................................................................... 632
Pause or Resume a Scan (Classic Interface) ............................................................ 633
Start or Stop a Scan (Classic Interface) ................................................................. 635
View Scans (Classic Interface) ................................................................................. 637
Edit a Scan Configuration (Classic Interface) ......................................................... 639
Change Scan Ownership (Classic Interface) ............................................................ 641
Update Scan Permissions (Classic Interface) ............................................................ 642
Copy a Scan Configuration (Classic Interface) ......................................................... 643
Move a Scan to the Trash Folder (Classic Interface) ................................................. 644
Delete a Scan (Classic Interface) ............................................................................. 645
Delete Scan Job (Classic Interface) .......................................................................... 646
Tenable-Provided Scanner Templates (Classic Interface) ........................................... 648
WAS Scan Templates (Classic Interface) ................................................................. 652
Agent Templates (Classic Interface) ................................................................. 710
Scan and Policy Settings (Classic Interface) .................................................. 712
Configure Scan Settings (Classic Interface) .................................................. 714
WAS Credentials (Classic Interface) ............................................................... 715
WAS Server-Based Authentication (Classic Interface) ..................................... 716
Configure WAS Login Form Authentication (Classic Interface) ....................... 718
WAS Cookie Authentication (Classic Interface) .............................................. 720
Configure WAS Selenium Authentication (Classic Interface) ......................... 724
Set Scan Permissions (Classic Interface) ....................................................... 727
Basic Settings for Scans (Classic Interface) ................................................... 728
Basic Settings for Policies (Classic Interface) ................................................. 736
Discovery Settings (Classic Interface) .......................................................... 743
Assessment Settings (Classic Interface) ........................................................ 753
Report Settings (Classic Interface) ............................................................... 767
Advanced Settings (Classic Interface) ............................................................ 769
Credentials (Classic Interface) ................................................................. 774
Add or Edit Managed Credentials for a Scan (Classic Interface) ..................... 777
WAS Web App Authentication (Classic Interface) ........................................... 780
Scan Folders (Classic Interface) .................................................................... 787
Manage Scan Folders (Classic Interface) ....................................................... 788
View Results for an Individual Scan (Classic Interface) ................................ 791
Change the Scan Read Status (Classic Interface) .......................................... 793
View Asset Details for an Individual Scan (Classic Interface) ......................... 794
View Vulnerability Details for an Individual Scan (Classic Interface) .......... 797
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Vulnerability Information</td>
<td>800</td>
</tr>
<tr>
<td>View Audit Details for an Individual Scan (Classic Interface)</td>
<td>802</td>
</tr>
<tr>
<td>View Audit Information</td>
<td>804</td>
</tr>
<tr>
<td>View Scan History Details (Classic Interface)</td>
<td>806</td>
</tr>
<tr>
<td>View Scan Notes (Classic Interface)</td>
<td>808</td>
</tr>
<tr>
<td>Export Scan Results (Classic Interface)</td>
<td>809</td>
</tr>
<tr>
<td>Policies (Classic Interface)</td>
<td>812</td>
</tr>
<tr>
<td>Create a Policy (Classic Interface)</td>
<td>814</td>
</tr>
<tr>
<td>Copy a Policy (Classic Interface)</td>
<td>815</td>
</tr>
<tr>
<td>Import a Policy (Classic Interface)</td>
<td>816</td>
</tr>
<tr>
<td>Export a Policy (Classic Interface)</td>
<td>817</td>
</tr>
<tr>
<td>Change Policy Ownership (Classic Interface)</td>
<td>818</td>
</tr>
<tr>
<td>Set Policy Permissions (Classic Interface)</td>
<td>819</td>
</tr>
<tr>
<td>Delete a Policy (Classic Interface)</td>
<td>820</td>
</tr>
<tr>
<td>Scanners (Classic Interface)</td>
<td>822</td>
</tr>
<tr>
<td>Link a Scanner (Classic Interface)</td>
<td>828</td>
</tr>
<tr>
<td>Modify Scanner Permissions (Classic Interface)</td>
<td>829</td>
</tr>
<tr>
<td>Enable or Disable a Scanner (Classic Interface)</td>
<td>830</td>
</tr>
<tr>
<td>Remove a Scanner (Classic Interface)</td>
<td>831</td>
</tr>
<tr>
<td>Download Managed Scanner Logs (Classic Interface)</td>
<td>832</td>
</tr>
<tr>
<td>Scanner Settings (Classic Interface)</td>
<td>834</td>
</tr>
<tr>
<td>Modify Scanner Settings (Classic Interface)</td>
<td>835</td>
</tr>
<tr>
<td>Scanner Groups (Classic Interface)</td>
<td>836</td>
</tr>
<tr>
<td>Create a Scanner Group (Classic Interface)</td>
<td>837</td>
</tr>
</tbody>
</table>
Edit a Scanner Group (Classic Interface) ........................................ 838
Delete a Scanner Group (Classic Interface) ..................................... 839
Networks (Classic Interface) .......................................................... 841
Create a Network (Classic Interface) ............................................. 843
Add a Scanner to a Network (Classic Interface) ............................... 845
Remove a Scanner from a Network (Classic Interface) ...................... 847
View or Edit a Network (Classic Interface) ..................................... 848
Move Assets to a Network (Classic Interface) ................................... 850
Delete Assets from a Network (Classic Interface) .............................. 852
Delete a Network (Classic Interface) ............................................. 854
Agents (Classic Interface) ............................................................. 855
Retrieve the Nessus Agent Linking Key (Classic Interface) ............... 857
Agent Settings (Classic Interface) .................................................. 858
Modify Agent Settings (Classic Interface) ....................................... 859
Agent Status (Classic Interface) ..................................................... 860
Filter Agents (Classic Interface) ................................................... 861
Unlink an Agent (Classic Interface) ............................................... 863
Export Agents (Classic Interface) .................................................. 865
Download Linked Agent Logs (Classic Interface) ............................. 867
Agent Groups (Classic Interface) ................................................... 869
Create an Agent Group (Classic Interface) ..................................... 870
Configure User Permissions for an Agent Group (Classic Interface) .... 871
Modify an Agent Group (Classic Interface) ..................................... 873
Delete an Agent Group (Classic Interface) ...................................... 875
Blackout Windows (Classic Interface) ................................................................. 876
Create a Blackout Window (Classic Interface) .................................................. 877
Modify a Blackout Window (Classic Interface) .................................................. 878
Delete a Blackout Window (Classic Interface) .................................................. 879

Settings .................................................................................................................. 880
General Settings ..................................................................................................... 881
Configure Your Severity Metric ............................................................................. 882
Configure Your SLA Settings .................................................................................. 884
Change the Language for Plugin Details .............................................................. 886
View Information about Your Tenable.io Instance ................................................ 888
View Information about Your Tenable.io Instance (Classic Interface) ................. 890
Recast/Accept Rules ............................................................................................... 891
View Recast/Accept Rules ...................................................................................... 894
Create a Recast Rule .............................................................................................. 895
Create an Accept Rule for a Plugin ........................................................................ 897
Edit a Recast or Accept Rule .................................................................................. 899
Delete a Recast or Accept Rule .............................................................................. 900
Recast Rules (Classic Interface) ............................................................................ 901
View Recast/Accept Rules (Classic Interface) ...................................................... 904
Create a Recast Rule (Classic Interface) .............................................................. 905
Edit a Recast Rule (Classic Interface) ................................................................. 908
Delete a Recast Rule (Classic Interface) .............................................................. 910
Create an Accept Rule (Classic Interface) ........................................................... 912
Delete an Accept Rule (Classic Interface) ............................................................ 915
<p>| User Roles | 1013 |
| User Role Permissions | 1015 |
| Tenable.io Password Requirements | 1022 |
| Create a User Account | 1023 |
| Edit a User Account | 1026 |
| Change Another User’s Password | 1028 |
| Configure SSO/SAML Authentication | 1029 |
| Assist a User with Their Account | 1031 |
| Generate Another User’s API Keys | 1032 |
| Unlock a User Account | 1033 |
| Disable a User Account | 1034 |
| Enable a User Account | 1036 |
| Manage User Access Authorizations | 1038 |
| Audit User Activity | 1039 |
| Delete a User Account | 1041 |
| Users (Classic Interface) | 1043 |
| Create a User Account (Classic Interface) | 1044 |
| Edit a User Account (Classic Interface) | 1046 |
| Configure Two-Factor Authentication (Classic Interface) | 1048 |
| Change a Password (Classic Interface) | 1050 |
| Generate API Keys (Classic Interface) | 1052 |
| Impersonate a User Account (Classic Interface) | 1054 |
| Disable a User Account (Classic Interface) | 1055 |
| Enable a User Account (Classic Interface) | 1056 |</p>
<table>
<thead>
<tr>
<th>User Groups</th>
<th>1057</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a User Group</td>
<td>1058</td>
</tr>
<tr>
<td>Edit a User Group</td>
<td>1060</td>
</tr>
<tr>
<td>Delete a Group</td>
<td>1062</td>
</tr>
<tr>
<td>Groups (Classic Interface)</td>
<td>1064</td>
</tr>
<tr>
<td>Create a Group (Classic Interface)</td>
<td>1065</td>
</tr>
<tr>
<td>Edit a Group (Classic Interface)</td>
<td>1066</td>
</tr>
<tr>
<td>Delete a Group (Classic Interface)</td>
<td>1068</td>
</tr>
<tr>
<td>Sensors Overview</td>
<td>1069</td>
</tr>
<tr>
<td>Cloud Sensors</td>
<td>1070</td>
</tr>
<tr>
<td>Linked Scanners</td>
<td>1074</td>
</tr>
<tr>
<td>View Linked Scanners</td>
<td>1077</td>
</tr>
<tr>
<td>Download Linked Scanner Logs</td>
<td>1078</td>
</tr>
<tr>
<td>Link a Sensor</td>
<td>1080</td>
</tr>
<tr>
<td>Regenerate a Linking Key</td>
<td>1085</td>
</tr>
<tr>
<td>View Sensor Details</td>
<td>1087</td>
</tr>
<tr>
<td>Edit Sensor Settings</td>
<td>1088</td>
</tr>
<tr>
<td>Sensor Settings</td>
<td>1090</td>
</tr>
<tr>
<td>Edit Sensor Permissions</td>
<td>1091</td>
</tr>
<tr>
<td>Enable or Disable a Sensor</td>
<td>1093</td>
</tr>
<tr>
<td>Remove a Sensor</td>
<td>1094</td>
</tr>
<tr>
<td>Scanner Groups</td>
<td>1095</td>
</tr>
<tr>
<td>Create a Scanner Group</td>
<td>1097</td>
</tr>
<tr>
<td>Modify a Scanner Group</td>
<td>1099</td>
</tr>
</tbody>
</table>
Configure User Permissions for a Scanner Group .................................................. 1102
Delete a Scanner Group .................................................................................... 1104
Add a Sensor to a Scanner Group ...................................................................... 1106
Remove a Sensor from a Scanner Group ............................................................ 1108
View Sensors in a Scanner Group ...................................................................... 1110
View All Scans for a Sensor ............................................................................... 1111
Agents .................................................................................................................. 1112
Retrieve the Nessus Agent Linking Key .............................................................. 1113
Download Linked Agent Logs ........................................................................... 1114
Restart an Agent .................................................................................................. 1116
Unlink an Agent ................................................................................................... 1118
Agent Settings .................................................................................................... 1120
Manage an Agent’s Settings ............................................................................... 1121
Edit Global Agent Settings ............................................................................... 1129
Agent Status ........................................................................................................ 1130
Export Agents ..................................................................................................... 1131
Agent Filters ........................................................................................................ 1133
Agent Groups ....................................................................................................... 1135
Create an Agent Group ....................................................................................... 1136
Add an Agent to an Agent Group ....................................................................... 1138
Edit an Agent Group ........................................................................................... 1140
Delete an Agent Group ....................................................................................... 1142
Remove an Agent from an Agent Group ............................................................ 1143
View Agents in an Agent Group ......................................................................... 1145
AWS Connector with Keyless Authentication (Discovery Only) ................................. 1192
Configure AWS for Keyless Authentication (Discovery Only) ................................ 1195
Create an AWS Connector with Keyless Authentication (Discovery Only) .................. 1198
AWS Connector with Key-based Authentication ......................................................... 1201
Configure AWS for Key-based Authentication ......................................................... 1203
Configure Linked AWS Accounts for Key-based Authentication ............................... 1205
Create an AWS Connector with Key-based Authentication ....................................... 1208
Google Cloud Platform Connector ........................................................................... 1210
Configure Google Cloud Platform (GCP) ................................................................. 1211
Create a Google Cloud Platform Connector ............................................................. 1216
Microsoft Azure Connector ....................................................................................... 1218
Configure Microsoft Azure ....................................................................................... 1219
Create Azure Application ......................................................................................... 1220
Obtain Azure Tenant ID (Directory ID) ..................................................................... 1226
Obtain Azure Subscription ID ................................................................................... 1228
Grant the Azure Application Reader Role Permissions ............................................. 1230
Link Azure Subscriptions ......................................................................................... 1236
Create a Microsoft Azure Connector .......................................................................... 1242
Launch a Connector Import Manually ...................................................................... 1245
Manage Existing Connectors .................................................................................... 1246
Launch a Connector Import Manually ...................................................................... 1247
View Connectors Details ......................................................................................... 1248
View Connector Event History .................................................................................. 1250
Edit a Connector ....................................................................................................... 1252
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete a Connector</td>
<td>1257</td>
</tr>
<tr>
<td>Analysis</td>
<td>1258</td>
</tr>
<tr>
<td>Lumin</td>
<td>1259</td>
</tr>
<tr>
<td>Lumin Metrics</td>
<td>1260</td>
</tr>
<tr>
<td>Improve Your Lumin Metrics</td>
<td>1270</td>
</tr>
<tr>
<td>Edit an ACR Manually</td>
<td>1272</td>
</tr>
<tr>
<td>Lumin Data Timing</td>
<td>1275</td>
</tr>
<tr>
<td>View the Lumin Dashboard</td>
<td>1277</td>
</tr>
<tr>
<td>Export the Lumin Dashboard Landing Page</td>
<td>1278</td>
</tr>
<tr>
<td>Export a Widget from the Lumin Dashboard</td>
<td>1279</td>
</tr>
<tr>
<td>Update the Lumin Industry Benchmark</td>
<td>1280</td>
</tr>
<tr>
<td>Exclude or Include Assets with Predicted Scores from your CES</td>
<td>1282</td>
</tr>
<tr>
<td>Lumin Dashboard Widgets</td>
<td>1284</td>
</tr>
<tr>
<td>View the CES Details Panel</td>
<td>1293</td>
</tr>
<tr>
<td>View Assessment Maturity Details</td>
<td>1299</td>
</tr>
<tr>
<td>View Remediation Maturity Details</td>
<td>1307</td>
</tr>
<tr>
<td>View Business Context/Tag Asset Details</td>
<td>1315</td>
</tr>
<tr>
<td>View Your Lumin External Risk Rating</td>
<td>1322</td>
</tr>
<tr>
<td>View Mitigations Details in Lumin</td>
<td>1326</td>
</tr>
<tr>
<td>Plugins for Mitigation Detection</td>
<td>1329</td>
</tr>
<tr>
<td>Export Mitigations</td>
<td>1332</td>
</tr>
<tr>
<td>Mitigations Export File Contents</td>
<td>1333</td>
</tr>
<tr>
<td>View and Download Exported Mitigations</td>
<td>1335</td>
</tr>
<tr>
<td>View Recommended Actions</td>
<td>1336</td>
</tr>
</tbody>
</table>
View Asset Vulnerabilities (Classic Interface) ................................................................. 1401
View Additional Asset Information (Classic Interface) ..................................................... 1402
Delete Assets (Classic Interface) ....................................................................................... 1403
Delete Assets from the Assets Table (Classic Interface) .................................................. 1404
Delete Assets from the Asset Detail Page (Classic Interface) ........................................... 1405
View Deleted Assets (Classic Interface) ............................................................................. 1406
Manage Asset Tags (Classic Interface) .............................................................................. 1407
Apply a Tag to an Asset (Classic Interface) ...................................................................... 1408
Remove a Tag from an Asset (Classic Interface) .............................................................. 1411
Create Tag Rules from Advanced Search Filters (Classic Interface) .............................. 1413
Filter the Assets Workbench by Tag (Classic Interface) ................................................... 1415

Vulnerabilities .................................................................................................................. 1417
CVSS vs. VPR .................................................................................................................. 1419
View Vulnerabilities by Plugin ......................................................................................... 1423
View Vulnerabilities by Asset .......................................................................................... 1425
View Vulnerabilities by Application in WAS .................................................................. 1426
View Vulnerability Details ............................................................................................... 1427
Vulnerability Details ......................................................................................................... 1428
Create an Accept Rule from Vulnerability Details ......................................................... 1432
Create a Recast Rule from Vulnerability Details .......................................................... 1434
View Plugin Output ......................................................................................................... 1436
Copy Plugin Output ......................................................................................................... 1437
View Plugin Attachments ................................................................................................. 1438
Export Vulnerability Data ............................................................................................... 1440
CSV Vulnerability Export Fields ................................................................. 1445
Vulnerability Filters ................................................................................. 1448
Application Filters in WAS ........................................................................ 1456
Vulnerability Severity Indicators ................................................................. 1457
Vulnerability States ..................................................................................... 1458
Vulnerabilities (Classic Interface) ................................................................. 1459
Vulnerabilities By Plugin (Classic Interface) ............................................... 1460
Vulnerabilities By Asset (Classic Interface) ............................................... 1464
Plugin Details (Classic Interface) ................................................................. 1467
Vulnerability States (Classic Interface) ......................................................... 1468
Solutions ...................................................................................................... 1469
View Solutions ............................................................................................. 1470
Export Solutions .......................................................................................... 1472
View Solution Details .................................................................................. 1474
Dashboards ................................................................................................... 1477
Vulnerability Management Overview Dashboard ........................................ 1478
WAS Dashboard ........................................................................................... 1484
CS Dashboard ............................................................................................... 1485
Configure CS Connectors to Import and Scan Images ............................... 1486
Configure an AWS ECR Connector to Import Images in CS .................... 1488
Configure a Local Connector to Import Images in CS ................................ 1490
View Container Details ............................................................................... 1493
View Scan Results for Container Images .................................................... 1499
Manage CS Image Repositories ................................................................. 1502
Delete an Image in CS ................................................................. 1504
Manage CS Policies ................................................................. 1505
Add a CS Policy ..................................................................... 1506
Edit a CS Policy ..................................................................... 1508
Delete a CS Policy ................................................................. 1510
CS Policy Condition Settings .................................................. 1512
Risk Metrics in CS ................................................................. 1513
View CS Data Usage ............................................................. 1515
Dashboard Synchronization in Classic and New Interface .......... 1517
View the Dashboards Page ...................................................... 1518
Tenable-Provided Dashboards .................................................. 1520
Export a Full Dashboard Landing Page ..................................... 1521
Export an Individual Dashboard Widget .................................. 1522
View an Individual Dashboard ............................................... 1523
View the Dashboard Template Library .................................... 1524
Create a Dashboard ............................................................... 1525
Preview a Dashboard ............................................................ 1528
Manage Dashboards ............................................................. 1529
Toggle the Grid and List Dashboards View ...................... 1530
Edit a Dashboard ................................................................. 1531
Set a Default Dashboard ...................................................... 1534
Rename a Dashboard ............................................................ 1535
Duplicate a Dashboard .......................................................... 1536
Filter a Dashboard ............................................................... 1537
Share a Dashboard ............................................................. 1539
Export a Dashboard .......................................................... 1541
Download an Available Export Download .............................. 1545
Delete a Scheduled Dashboard Export Configuration ............. 1546
Delete a Dashboard Export Download .................................. 1547
Delete a Dashboard ............................................................ 1548
Manage Widgets .................................................................. 1549
View the Widget Library ....................................................... 1550
Toggle the Grid and List Widgets View ................................. 1552
Delete a Widget from the Widget Library .............................. 1553
Create a Custom Widget ....................................................... 1554
Edit a Custom Widget ........................................................ 1557
Add a Widget to a Dashboard .............................................. 1558
Configure a Widget ............................................................ 1560
Duplicate a Widget ............................................................. 1563
Rename a Widget ............................................................... 1564
Delete a Widget from a Dashboard ...................................... 1565
Dashboards and Workbenches (Classic Interface) .................. 1566
Web Applications Workbench (Classic Interface) ................. 1567
PCI ASV (Classic Interface) ................................................ 1569
Health and Status (Classic Interface) .................................... 1570
Dashboard Templates (Classic Interface) ............................... 1572
Create a Dashboard (Classic Interface) ................................. 1573
Dashboard Settings (Classic Interface) ................................. 1574
Chart Definitions (Classic Interface) ................................................................. 1575
Manage Dashboards (Classic Interface) ............................................................ 1577
Configure a Dashboard (Classic Interface) ....................................................... 1578
Configure a Dashboard Component (Classic Interface) ................................... 1581
Set a Default Dashboard or Workbench (Classic Interface) ........................... 1589
Filter the Vulnerabilities or Assets Workbench (Classic Interface) ............... 1591
Filter the WAS Workbench (Classic Interface) ................................................. 1593
Delete a Dashboard (Classic Interface) ............................................................ 1594
Export a Workbench (Classic Interface) ........................................................... 1596
  Export a Custom Dashboard (PNG) (Classic Interface) ............................... 1598
  Export a Custom Dashboard (PDF) (Classic Interface) ............................... 1602
Schedule a Custom Dashboard Export (Classic Interface) ............................ 1603
Advanced Saved Search (Classic Interface) ...................................................... 1606
Modify a Custom Dashboard Chart (Classic Interface) .................................... 1618

Reports (Classic Interface) .............................................................................. 1619
Reports Workflow (Classic Interface) ............................................................... 1621
Report Settings (Classic Interface) ................................................................. 1622
Report Templates (Classic Interface) ............................................................... 1626
Manage Reports (Classic Interface) ................................................................. 1638
  Create a New Report (Classic Interface) ....................................................... 1639
  Edit an Existing Report (Classic Interface) ................................................. 1643
  Run a Report (Classic Interface) ................................................................. 1645
  View Report Results (Classic Interface) ...................................................... 1646
  Delete a Report (Classic Interface) .............................................................. 1649
Welcome to Tenable.io

Tenable.io® allows security and audit teams to share multiple Nessus, Nessus Agent, and Nessus Network Monitor scanners, scan schedules, scan policies, and scan results among an unlimited set of users or groups.

Tenable.io Vulnerability Management

Video: Introduction to Tenable.io

Get Started with Vulnerability Management

By making different resources available for sharing among users and groups, Tenable.io provides endless possibilities for creating customized workflows for vulnerability management programs, regardless of any of the numerous regulatory or compliance drivers that demand keeping your business secure.

Tenable.io can schedule scans, push policies, view scan findings, and control multiple Nessus scanners from the cloud. This enables the deployment of Nessus scanners throughout networks to both public and private clouds as well as multiple physical locations.

Tenable Lumin

Get Started with Tenable Lumin

Lumin features augment Tenable.io Vulnerability Management data. Use Lumin to quickly and accurately assess your Cyber Exposure risk and compare your health and remediation performance to other Tenable customers in your Salesforce industry and the larger population.

Lumin correlates raw vulnerability data with asset business criticality and threat context data to support faster, more targeted analysis workflows than traditional vulnerability management tools.

Tenable.io Web Application Scanning

Video: Introducing Tenable.io Web Application Scanning

Get Started with Tenable.io Web Application Scanning
Tenable.io Web Application Scanning offers significant improvements over the existing Web Application Tests policy template provided by the Nessus scanner, which is incompatible with modern web applications that rely on Javascript and are built on HTML5. This leaves you with an incomplete understanding of your web application security posture.

Tenable.io Web Application Scanning provides comprehensive vulnerability scanning for modern web applications. Tenable.io Web Application Scanning’s accurate vulnerability coverage minimizes false positives and false negatives, ensuring that security teams understand the true security risks in their web applications. The product offers safe external scanning that ensures production web applications are not disrupted or delayed, including those built using HTML5 and AJAX frameworks.

**Tenable.io Container Security**

*Video:* Introducing Tenable.io Container Security

**Get Started with Tenable.io Container Security**

Tenable.io Container Security stores and scans container images as the images are built, before production. It provides vulnerability and malware detection, along with continuous monitoring of container images. By integrating with the continuous integration and continuous deployment (CI/CD) systems that build container images, Tenable.io Container Security ensures every container reaching production is secure and compliant with enterprise policy.

**Tenable.io API**

*See the API*

The Tenable.io API can be leveraged to develop your own applications using various features of the Tenable.io platform, including scanning, creating policies, and user management.
Get Started with Vulnerability Management

Use the following getting started sequence to configure and mature your Tenable.io Vulnerability Management deployment.

1. **Prepare**
2. **Install**
3. **Configure Scans**
4. **Refine**
5. **Expand**

**Prepare**

Before you begin, learn about Tenable.io and establish a deployment plan and analysis workflow to guide your configurations.

To establish a deployment plan and analysis workflow:

1. Review principles of the TCP/IP internet protocol suite. Tenable.io documentation assumes you have knowledge of basic networking concepts and principles.
2. Get your Tenable.io access information and starter account credentials from your Tenable representative.
3. If necessary, access Tenable Support and training resources for Tenable.io, including:
   - the Professional Services [Scan Strategy](#) guide.
4. Design a deployment plan by identifying your organization's objectives and analyzing your network topology. Consider Tenable-recommended best practices for your environment.

For more information about environment requirements, see the guidelines provided for your scanner (Nessus, Nessus Agent, or NNM) in the [General Requirements Guide](#). For more information about supported browsers for Tenable.io, see [System Requirements](#).
If you are a Professional Services customer, contact your Tenable representatives for additional guidance.

5. Design an internal scanning and external scanning plan. Identify the scans you intend to run and ensure that you have sufficient network coverage.

If you are a Professional Services customer, contact your Tenable representatives for additional guidance.

6. Design an analysis workflow. Identify key stakeholders in your management and operational groups, considering the data you intend to share with each stakeholder.

If you are a Professional Services customer, contact your Tenable representatives for additional guidance.

Install

Install your scanners and link them to Tenable.io.

To install your scanners and link them to Tenable.io:

1. Log in to the Tenable.io web interface:
   a. In a supported web browser, navigate to https://cloud.tenable.com/.
      
      The Tenable.io login page appears.
   b. Type the **User name** and **Password** provided by Tenable.
   c. Click **Sign In**.
      
      The Tenable.io interface appears.

   **Tip:** Tenable.io is introducing the new Tenable.io interface in a rolling fashion. For more information about the classic interface or new interface, see [Navigate Tenable.io (Classic Interface)](#) or [Navigate Tenable.io (New Interface)](#).

2. If your deployment plan includes Nessus scanners, set up your virtual environments or install Nessus on your hardware, as described in [Install Nessus](#) in the **Nessus User Guide**.

   Then, link your first Nessus scanner to Tenable.io, as described in [Link a Sensor](#).
3. If your deployment plan includes Nessus Agents, set up your virtual environments or install agents on your hardware, as described in Install Nessus Agents in the Nessus Agent Deployment and User Guide.

Then, link your first agent to Tenable.io, as described in Link a Sensor.

4. If your deployment plan includes NNM, set up your virtual environments or install NNM on your hardware, as described in Install NNM in the Nessus Network Monitor User Guide.

Then, configure NNM to communicate with Tenable.io, as described in Configure NNM in the Nessus Network Monitor User Guide.

5. Create access groups to manage view and scan permissions for assets and targets, as described in Create an Access Group.

6. Create user accounts and user groups, as described in Create a User Account and Create a Group.

7. Create exclusion lists, as described in Create an Exclusion.

Configure Scans

Configure and run basic scans to begin evaluating the effectiveness of your deployment plan and analysis workflow.

To configure and run basic scans:

1. If your deployment plan includes more than one Nessus scanner, install and link your other Nessus scanners.

Then, configure your first active scan using the Basic Network Scan template:

   a. Create a scanner group, as described in Create a Scanner Group.
   
   b. Create a scan using the Basic Network Scan template, as described in Create a Scan.

2. If your deployment plan includes more than one NNM, install and link your other NNM scanners.
3. If your deployment plan includes more than one Nessus Agent, install and link your other agents.

Then, configure your first agent scan using the **Basic Agent Scan** template:

   a. Create an agent group, as described in [Create an Agent Group](#).

   b. Create an agent scan using the **Basic Agent Scan** template, as described in [Create a Scan](#).

4. Launch your first Nessus scan and agent scan, as described in [Launch a Scan](#).

5. Set up asset discovery with connecters, Professional Services integrations, or integrated products. For more information, see [Connectors](#), the [Custom Integration Services](#) page, or the [Integration Guides](#) section of the [Tenable.io Documentation](#) page.

6. Confirm your Nessus scan and agent scan completed, accessing all targeted areas of your network. Review your discovered assets to assess your knowledge of your network.

7. Configure managed credentials, scan-specific credentials, or policy-specific credentials for a Nessus scan, as described in [Credentials](#).

   For more information about configuring and troubleshooting credentialed scans, see [Nessus Credentialed Checks](#).

8. Launch your credentialed Nessus scan and credentialed agent scan, as described in [Launch a Scan](#).

9. Confirm your credentialed scan completed, accessing all targeted areas of your network.

   Tenable recommends frequently reviewing your scan results and scan coverage. You may need to modify your scan configurations to suit your organization’s objectives and reach all areas of your network.

### Refine

Configure other features, if necessary, and refine your existing configurations.

To configure/refine configurations:
1. If you want to allow other user accounts or user groups to access objects, share the objects with user accounts or user groups:
   - Set permissions on a report, as described in Modify an Existing Report.
   - Set permissions on a scan, as described in Basic Settings.
   - Set permissions on a sensor, as described in Modify Sensor Permissions.
   - Set permissions on an agent group, as described in Modify an Agent Group.
   - Set permissions on a target group, as described in Edit a Target Group.

2. View your individual scan results in the Scans views, as described in View Individual Scan Details.

3. View your aggregated scan results in the Vulnerabilities and Assets views, as described in Vulnerabilities and Assets.

4. Create saved searches for your Vulnerabilities and Assets views, as described in Saved Search.

5. Create a template-based or custom dashboard, as described in Create a Dashboard.

6. Export the dashboard, as described in Export a Dashboard.

7. Create recast rules and accept rules, as described in Recast Rules.

8. If you want to assess your Cyber Exposure, obtain a Lumin license.
   For more information about Lumin, see Tenable Lumin.

9. If you want to perform web application scanning, obtain a Tenable.io Web Application Scanning license.
   For more information about Tenable.io Web Application Scanning, see the Tenable.io Web Application Scanning User Guide.

10. If you want to evaluate risk on your containers, obtain a Tenable.io Container Security license.
    For more information about Tenable.io Container Security, see the Tenable.io Container Security User Guide.
11. Consider product integrations, including custom integrations provided by Professional Services.

12. Engage with Professional Services for ongoing deployment support and refinement.

Expand

Review and mature your deployment plan and analysis workflow.

To review and mature your deployment plan and analysis workflow:

- Conduct weekly meetings to review your organization's responses to identified vulnerabilities.
- Conduct weekly management meetings to oversee your teams executing the analysis workflow.
- Review your scan scheduling settings and consider revising.
- Review your scan results and scan coverage. You may need to modify your scan configurations to suit your organization's objectives and reach all areas of your network.
- Optimize and operationalize your custom dashboards to meet the needs of individual user account holders.
- Consider API integrations, as described in the [Tenable.io API Documentation](https://tenable.com).
Get Started with Lumin

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

You can use Tenable Lumin to quickly and accurately assess your Cyber Exposure risk and compare your health and remediation performance to other Tenable customers in your Salesforce industry and the larger population. Lumin correlates raw vulnerability data with asset business criticality and threat context data to support faster, more targeted analysis workflows than traditional vulnerability management tools.

Tenable recommends the following to get started with Lumin data and functionality.

License and Enable

Acquire a Lumin license and enable Lumin in Tenable.io.

1. To add Lumin to your Tenable.io license, contact your Tenable representative.

2. In your web browser, disable features that may prevent you from enabling Lumin:
   - Ad blocker extensions
   - Do Not Track (Mozilla Firefox, Google Chrome, Apple Safari, or Microsoft Internet Explorer)
   - Protected Mode (Microsoft Internet Explorer)

   **Tip:** You can re-enable these features after you fully enable Lumin.

3. Log in to Tenable.io, as described in [Log In to Tenable.io](#).

   The Lumin welcome window appears.

4. Follow the wizard to fully enable Lumin.

   The Lumin dashboard appears.

Prepare

Generate data and learn about Lumin terminology.
### Tenable.io Only

1. Run an authenticated assessment scan in Tenable.io to [generate vulnerability data](#).

   **Note:** You must run scans to start seeing data in Lumin views; Lumin displays scan result data generated after you licensed Lumin. For more information, see [Lumin Data Timing](#).

2. Create tags in Tenable.io to [add business context to your assets](#).

3. Review the [metrics terminology](#) to understand Vulnerability Priority Rating (VPR) and Asset Criticality Rating (ACR) values and how they impact your Asset Exposure Score (AES), Assessment Maturity grade, and Cyber Exposure Score (CES).

4. Allow sufficient time for your metrics to calculate. For more information, see [Lumin Data Timing](#).

### Tenable.sc + Tenable.io Lumin

1. Sync repositories to Lumin from Tenable.sc. All [vulnerability data](#) is synced immediately.

   **Note:** Lumin does not support third-party integration data.

2. Create assets in Tenable.sc to [add business context to your assets](#).

3. Configure [Tenable.sc to Lumin synchronization](#).

   Allow sufficient time for the synchronization to complete. For more information, see [Lumin Data Timing](#).

4. View your assets as business context tags in Tenable.io. For more information, see [Manage Asset Tags](#).

5. Review the [metrics terminology](#) to understand Vulnerability Priority Rating (VPR) and Asset Criticality Rating (ACR) values and how they impact your Asset Exposure Score (AES), Assessment Maturity grade, and Cyber Exposure Score (CES).

6. Allow sufficient time for your metrics to calculate. For more information, see [Lumin Data Timing](#).

### Assess Your Exposure

**Note:** All Lumin data reflects all assets within the organization’s Tenable.io instance.
Review your CES and perform vulnerability management analysis.

1. Use the Lumin dashboard to understand your CES and access details pages.
   - **Cyber Exposure Score** widget – How does your overall risk compare to other Tenable customers in your Salesforce industry and the larger population?
   - **Cyber Exposure Score Trend** widget – How has the overall risk for your entire organization changed over time?
   - **Assessment Maturity** widget – How frequently and thoroughly are you scanning your assets?
   - **Remediation Maturity** widget – How quickly and thoroughly are you remediating vulnerabilities on your assets?
   - **Reduce Cyber Exposure Score** widget – What would the impact be if you addressed all of your top 20 recommended actions?
   - **Asset Criticality Rating Breakdown** widget – How critical are your assets?
   - **Asset Scan Distribution** widget – What types of scans have run on your assets?
   - **Mitigations** widget – What endpoint protection agents are running on your assets?
   - **Cyber Exposure Score by Business Context/Tag** widget – How do assets with different tags (unique business context) compare?

2. To browse the most critical vulnerabilities on your network, sort your vulnerabilities by VPR.

3. To browse the most critical assets on your network, sort your assets by ACR.

**Customize Your ACR Values**

Review the Tenable-provided ACR values and customize them to reflect the unique infrastructure or concerns of your organization.

1. Use the Assets page to review the Tenable-provided ACR values for your assets.
   - Do any of your assets have ACR values that seem too high for the relative criticality of that asset?
• Do any of your assets have ACR values that seem too low for the relative criticality of that asset?

2. If necessary, manually customize your asset ACR values.

Lower Your CES and AES

You must address vulnerabilities on your network to lower your CES and AES.

1. View lists of Tenable-recommended action items:
   • Top recommended actions for all assets on your network.
     Export your top recommended actions, as necessary.
   • Top recommended actions for a group of assets on your network.
     Export your top recommended actions, as necessary.
   • All solutions on your network.
     Export your solutions, as necessary.

2. Follow the recommendations and take steps to address the vulnerabilities on your network.

Mature

Mature your vulnerability management strategy.

• Continue monitoring and addressing vulnerabilities to lower your CES and AES.

• Continue exporting and sharing recommended actions (solutions) data with others in your organization to refine your vulnerability management strategy.
Get Started with WAS

Use the following getting started sequence to configure and manage your Tenable.io Web Application Scanning deployment.

1. **Prepare**
2. **Install**
3. **Configure Scans**
4. **Refine**

**Prepare**

Before you begin, learn about Tenable.io Web Application Scanning and establish a deployment plan and analysis workflow to guide your implementation and configurations.

To establish a deployment plan and analysis workflow:

1. Review principles of the TCP/IP internet protocol suite. Tenable.io Web Application Scanning documentation assumes you have knowledge of basic networking concepts and principles.

2. Review principles of web application management and security. Tenable.io Web Application Scanning documentation assumes you have knowledge of web application management concepts and principles.

3. Get your Tenable.io Web Application Scanning access and license information and credentials from your Tenable representative.

4. Develop a deployment plan based on the following:
   - **Your organization's security policies** — Determine whether the policies allow you to store scanning data in Tenable.io Web Application Scanning, or require that you store data on your premises.
   - **How you manage and access the assets that host your web applications** — Determine the following about your web application assets:
• Which web applications you want to include in your scanning strategy.

• Whether these web applications can be accessed via publicly available sites or only on internal sites (for example, behind a firewall, on a staging site, deployed within a third-party cloud computing service).

5. Review the Tenable.io and Tenable.io Web Application Scanning requirements and ensure your machine and system meet the requirements.

Install

Tenable.io Web Application Scanning is configured with region-specific cloud scanners. You do not need to install additional scanners if your web application analysis scope includes only publicly available assets.

If your web applications are not available publicly, your installation plan depends on where your web applications run, as well as your organization’s data storage needs.

• If you want to analyze web applications that are available only internally, you must obtain and install the Tenable Core + Tenable.io Web Application Scanning platform and application package.

  For more information, see the Tenable Downloads site and the Tenable Core + Web Application Scanning User Guide.

• If you want to analyze web applications deployed within Microsoft Azure, you must provision a Tenable Core Web Application Scanner (BYOL) instance.

  For more information, see the Microsoft Azure Integration Guide.

Configure Scans

After you prepare your analysis workflow and determine which web application assets are in scope, you can configure and run scans on those assets.

Tenable recommends that you first run high-level overview scans to help you determine which settings you want to configure for your more in-depth scans.

Note: With a Tenable.io Web Application Scanning trial license, you can run up to five scans concurrently using your cloud scanners. You can run any number of scans concurrently using on-premises scanners.
To configure and run overview scans:

1. Do one of the following:
   - To perform an overview scan to determine which web application targets Tenable.io Web Application Scanning scans by default, create a scan using the **Overview scan template**.
   - To perform an overview scan to determine if your web application is compliant with common security industry standards, create a scan using the **Config Audit scan template**.

   **Note:** The Tenable-provided scan templates for overview scans do not require authentication. However, the plugin results from these scans can help you identify the types of credentials your web applications require for more in-depth scans.

2. Review the **scan results**, along with your scanning strategy, and determine which configuration settings you want to adjust when you run your standard web application scans.

To configure and run standard scans:

1. **Create a scan** using the template that best matches your assessment needs:
   - To perform a comprehensive vulnerabilities scan, select the **Scan** template.
   - To perform a scan to determine if your web application appropriately implements SSL/TLS public key encryption, select the **SSL TLS** template.

2. (Optional) Configure your scan settings, including **user permissions**, and **plugin** settings.

   **Note:** You can also configure your credentials options in standard scans. However, you need to add credentials only if your web application requires them for authentication.

3. **Launch** the scan.

4. Monitor the scan status.

5. **View** and analyze your scan results.

Refine

Configure other features, if necessary, and refine your existing configurations.

To configure/refine your configurations:
1. Further adjust your current scan settings, including user permissions, and plugin settings.

2. If you want to add credentials to your scan, add the appropriate credentials type:
   - If the scan must authenticate to the web application using methods required by your server's HTTP protocol, add HTTP Server-Based authentication.
   - If the scan must authenticate to the web application using methods required by the web application, add Web App authentication.

3. If you want to change basic scan settings, including the schedule, scanner used, or user permissions, adjust the Basic Settings in WAS Scans in the scan configuration.

4. If you want to widen or narrow the scope of URL targets your scan crawls, adjust the Scope Settings in WAS Scans in the scan configuration.

5. If you want to increase or decrease your scan intensity, adjust the Assessment Settings in WAS Scans in the scan configuration.

6. If you want improve your scan performance, adjust the Advanced Settings in WAS Scans in the scan configuration.
Get Started with CS

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Complete the following tasks in the order listed to get started with Tenable.io Container Security.

1. Activate your account and log in to the web portal.
2. Review the requirements described in CS Requirements.
3. Review the user permissions assigned to each user role.
4. Generate API Keys for the Tenable.io API.
5. Import and scan your container images, as described in CS Scanning Overview.
6. Navigate the Tenable.io Container Security dashboard to view and manage your scan data.

Note: Tenable.io Container Security imports and rescans your images at regular intervals, beginning when you first import and scan the images.
System Requirements

Display Settings

Minimum screen resolution: 1440 x 1024

Supported Browsers

- Google Chrome (40+)
- Apple Safari (8+)
- Mozilla Firefox (38+)
- Microsoft Edge (Chromium)
WAS Requirements

Hardware Requirements

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Hardware Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAS Scanning up to 4 concurrent web applications</td>
<td><strong>CPU</strong>: (4) 2 GHz cores</td>
</tr>
<tr>
<td></td>
<td><strong>Core Ram</strong>: 16GB RAM</td>
</tr>
<tr>
<td></td>
<td><strong>Hard Drive</strong>: 25GB</td>
</tr>
</tbody>
</table>

Application Requirements

All applications you want to scan must be compatible with Google Chrome, because Tenable.io Web Application Scanning uses Google Chrome browsers to run certain plugins.
CS Requirements

You can access Tenable.io Container Security from any machine that meets the System Requirements described in the Tenable.io Vulnerability Management User Guide.

Supported Container Image Formats

Tenable.io Container Security supports the following image formats:

<table>
<thead>
<tr>
<th>Import and Scan Method</th>
<th>Supported Image Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Push a Container Image to Tenable.io Container Security</td>
<td>Docker images</td>
</tr>
<tr>
<td>Configure Connectors to Import and Scan Images</td>
<td>Docker images</td>
</tr>
<tr>
<td>Configure and Run the Tenable.io Container Security Scanner</td>
<td>• Docker images</td>
</tr>
<tr>
<td></td>
<td>• Open Containers Initiative (OCI) images</td>
</tr>
</tbody>
</table>

Supported Registries

The container registries that Tenable.io Container Security supports depends on the method you use to import and scan images.

Tenable tests and verifies successful import and scanning for the following registries:

<table>
<thead>
<tr>
<th>Import and Scan Method</th>
<th>Supported Image Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Push a Container Image to Tenable.io Container Security</td>
<td>Docker registry</td>
</tr>
<tr>
<td>Configure Connectors to Import and Scan Images</td>
<td>• Amazon Web Service (AWS) Elastic Container Registry (ECR)</td>
</tr>
<tr>
<td></td>
<td>• JFrog Artifactory registry</td>
</tr>
<tr>
<td></td>
<td>• Docker registry</td>
</tr>
</tbody>
</table>
Configure and Run the Tenable.io Container Security Scanner

- Amazon Web Service (AWS) Elastic Container Registry (ECR)
- Azure Container registry
- Docker registry
- Docker Hub registry
- Google Cloud Platform (GCP) Google Container Registry (GCR)
- Harbor registry
- JFrog Artifactory registry
- Nexus Repository Manager registry

**Note:** Tenable.io Container Security supports importing and scanning from tested and verified registries that are compatible with Docker Registry API version 2.0. If you choose to import and scan images from registries that have not been tested and verified, Tenable Support cannot assist with your configurations.

**Port Requirements**

The machine where you run Tenable.io Container Security must allow outbound traffic to TCP port 443 for communications with the cloud.tenable.com server.
Vulnerability Management Licenses

Your Tenable.io Vulnerability Management instance has a licensed asset limit, which determines the number of assets you can scan for vulnerabilities. If you exceed your license limit, you can temporarily continue to use Tenable.io to scan your assets before adjusting your license as needed.

You can view your license information to see how many assets are currently being counted against your Tenable.io license. You can use this information to evaluate how effectively you are using your asset licenses.

To understand licenses, see the following sections:

- [How Assets are Counted](#)
- [Reclaiming Licenses](#)
- [Plugins Excluded from the License Limit](#)

**Note:** You can use the **IsLicensed (VM)** advanced search filter to view assets that currently count against your Tenable.io license. For more information, see [Filter a Table](#).

### How Assets are Counted

Tenable.io analyzes multiple asset attributes, not just IP addresses, to identify an asset. For more information on how Tenable.io identifies an asset, see the [Tenable.io FAQ](#).

Assets are counted towards your license limit depending on how Tenable.io discovers, or *sees*, the asset. In general, an asset does not count against your license limit unless it has been assessed for vulnerabilities.

<table>
<thead>
<tr>
<th>Assets Counted</th>
<th>Assets Not Counted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conditions where an asset <em>counts</em> towards your license limit can include:</td>
<td>Conditions where an asset <em>does not count</em> towards your license limit can include:</td>
</tr>
<tr>
<td>- An active scan.</td>
<td>- A scan configured with the Host Discovery template or configured to use only the discovery plugins.</td>
</tr>
<tr>
<td>- An agent scan.</td>
<td>- An import of asset data that does not</td>
</tr>
</tbody>
</table>
a scan result from Nessus Professional).

- A connector with Frictionless Assessment.

contain information on vulnerabilities (for example, ServiceNow data).

- A linked instance of Nessus Network Monitor running in discovery mode.

- A discovery-only connector, until and unless the asset is scanned for vulnerabilities.

Reclaiming Licenses

When Tenable.io reclaims a license, that license becomes available for a different asset. Tenable.io reclaims licenses in the following scenarios:

- When a licensed asset has not been scanned for 90 days, it ages out of the license count.

- If an asset was discovered through connectors and subsequently became licensed, the asset license is reclaimed the day after the asset is terminated. You can observe this event via the connector.

You can monitor licenses that are expected to be reclaimed in your License Information.

Plugins Excluded from the License Limit

The following plugins do not count towards the license limit.

Note: Plugin IDs are static, but Tenable.io occasionally updates plugin names. For the latest information on plugins, see https://www.tenable.com/plugins.

Nessus Plugins set through Discovery Settings

<table>
<thead>
<tr>
<th>Nessus Plugin ID</th>
<th>Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>10180</td>
<td>Port scanners</td>
</tr>
<tr>
<td>10335</td>
<td>Port scanners</td>
</tr>
<tr>
<td>11219</td>
<td>Port scanners</td>
</tr>
<tr>
<td>Nessus Plugin ID</td>
<td>Family</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>45590</td>
<td>General</td>
</tr>
<tr>
<td>54615</td>
<td>General</td>
</tr>
<tr>
<td>12053</td>
<td>General</td>
</tr>
<tr>
<td>11936</td>
<td>General</td>
</tr>
<tr>
<td>10287</td>
<td>General</td>
</tr>
<tr>
<td>22964</td>
<td>Service Detection</td>
</tr>
<tr>
<td>11933</td>
<td>Settings</td>
</tr>
<tr>
<td>87413</td>
<td>Settings</td>
</tr>
<tr>
<td>19506</td>
<td>Settings</td>
</tr>
<tr>
<td>33812</td>
<td>Settings</td>
</tr>
<tr>
<td>33813</td>
<td>Settings</td>
</tr>
</tbody>
</table>

Nessus Network Monitor Plugins

<table>
<thead>
<tr>
<th>Nessus Network Monitor Plugin ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Open Ports</td>
</tr>
<tr>
<td>12</td>
<td>Host TTL discovered</td>
</tr>
<tr>
<td>18</td>
<td>Protocols Information</td>
</tr>
<tr>
<td>19</td>
<td>VLAN IDs</td>
</tr>
<tr>
<td>----</td>
<td>----------</td>
</tr>
<tr>
<td>20</td>
<td>IPv6 Tunnel Information</td>
</tr>
<tr>
<td>113</td>
<td>VXLAN Information</td>
</tr>
<tr>
<td>132</td>
<td>Host Attribute Enumeration</td>
</tr>
</tbody>
</table>
WAS Licenses

Your Tenable.io Web Application Scanning instance has a licensed asset limit that determines the number of web application assets you can scan for vulnerabilities. If you exceed your limit, you can temporarily continue to use Tenable.io Web Application Scanning to scan your assets before adjusting your license as needed.

You can view your license information to see how many assets are currently counted against your Tenable.io Web Application Scanning license. You can use this information to evaluate how effectively you are using your asset licenses.

How Assets are Counted

Tenable.io Web Application Scanning determines asset count by the number of fully-qualified domain names (FQDNs) that Tenable.io Web Application Scanning successfully scans for your user account. An asset does not count against your license limit until Tenable.io Web Application Scanning has successfully scanned the asset for vulnerabilities.

FQDNs appear on your license as complete URLs. Per the RFC-3986 internet standard, each FQDN includes the following components and format:

```
hostname.parent domain.top-level domain
```

When you specify a web application target in a scan, Tenable.io Web Application Scanning counts that target as a separate asset if any component of the FQDN differs from that of another scanned target or previously scanned asset. Multiple targets with different paths appended to the FQDN count as a single asset, as long as all components of the FQDNs match.

The following targets would count toward a single asset in Tenable.io Web Application Scanning:

```
hostname.parent domain.top-level domain/path1
hostname.parent domain.top-level domain/path2
hostname.parent domain.top-level domain/path2/path3
```

**Note:** When a licensed target has not been scanned for 90 days, it ages out of the licensed count.

Example
In this example, Tenable.io Web Application Scanning successfully scans the following target and counts it toward your licensed asset limit.

https://www.example.com

In the following table, targets in the first column would count as the same asset as the example asset, and targets in the second column would count as separate assets from the example.

<table>
<thead>
<tr>
<th>Same Asset</th>
<th>Separate Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>(all FQDN components match)</td>
<td>(FQDN components do not all match)</td>
</tr>
<tr>
<td>• <a href="https://example.com/welcome">https://example.com/welcome</a></td>
<td>• <a href="https://en.example.com">https://en.example.com</a> (different hostname)</td>
</tr>
<tr>
<td>• <a href="https://example.com/welcome/get-started">https://example.com/welcome/get-started</a></td>
<td>• <a href="https://www.ex-ample.com">https://www.ex-ample.com</a> (different parent domain)</td>
</tr>
<tr>
<td>• <a href="https://example.com/welcome/get-started/create-new-user">https://example.com/welcome/get-started/create-new-user</a></td>
<td>• <a href="https://www.example.org">https://www.example.org</a> (different top-level domain)</td>
</tr>
</tbody>
</table>
Log in to Tenable.io

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

Before you begin:

- Obtain credentials for your Tenable.io user account.

  **Note:** If you are an administrator logging in to your Tenable.io instance for the first time, Tenable provides your first-time credentials during setup. After you log in for the first time, you can set your new password. If you are logging in to Tenable.io after initial setup, your username is the email address you used to register for your Tenable.io account.

- Review the [System Requirements](#) in the *General Requirements User Guide* and confirm that your computer and browser meet the requirements.

To log in to Tenable.io:

1. In a supported browser, navigate to [https://cloud.tenable.com](https://cloud.tenable.com).
   
The Tenable.io login page appears.

2. In the username box, type your Tenable.io username.

3. In the password box, type the Tenable.io password you created during registration.

4. (Optional) To retain your username for later sessions, select the **Remember Me** check box.

5. Click **Sign In**.

   The Tenable.io landing page appears. In Tenable.io Vulnerability Management, the landing page displays your [default dashboard](#).

   **Note:** Tenable.io logs you out after a period of inactivity (typically, 30 minutes). In FedRAMP environments, Tenable.io is required to log you out after 15 minutes of inactivity.
Navigate Tenable.io (New Interface)

Tip: This topic describes navigation in the new Tenable.io. For information about the classic interface, see Navigate Tenable.io (Classic Interface).

For most features, you can access the new interface in addition to the classic interface. Tenable is introducing the remaining features in the new interface in a rolling fashion. For a list of features currently available in the new interface, see Transition to the New Interface or Transition to the New WAS Interface. For announcements of features in the new interface, see Tenable.io release notes.

For more information, see the following topics:
Transition to the New Interface

Welcome to the new interface!

Tenable designed this new interface to improve the efficiency and ease of your workflow as you configure scans and analyze scan results.

The system requirements are the same for both classic and new interfaces.

Feature Parity

The table below lists which tasks are supported in each interface.

<table>
<thead>
<tr>
<th>Task</th>
<th>Classic</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get Started</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Navigate the interface</td>
<td>Navigate Tenable.io (Classic Interface)</td>
<td>Navigate Tenable.io (New Interface)</td>
</tr>
<tr>
<td>Save searches</td>
<td>Advanced Save Search</td>
<td>Saved Search</td>
</tr>
<tr>
<td>Scans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create or edit a scan config</td>
<td>Create a Scan</td>
<td>Create a Scan</td>
</tr>
<tr>
<td>Import a scan</td>
<td>Import a Scan</td>
<td>Import a Scan</td>
</tr>
<tr>
<td>Launch a scan</td>
<td>Launch a Scan</td>
<td>Launch a Scan</td>
</tr>
<tr>
<td>Pause or resume a scan</td>
<td>Pause or Resume a Scan</td>
<td>Pause or Resume a Scan</td>
</tr>
</tbody>
</table>

Note: In the classic interface, the Legacy Web App Scan template appears in the Web Application tab of the Tenable-provided scan templates. In the new interface, this template appears in the Scanners tab of the templates.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Web App</th>
<th>Desktop Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop a scan</td>
<td>Stop a Scan</td>
<td>Stop a Running Scan</td>
</tr>
<tr>
<td>View your scans</td>
<td>View Scans</td>
<td>View Scans</td>
</tr>
<tr>
<td>Edit scan configurations</td>
<td>Edit a Scan Configuration</td>
<td>Edit a Scan Configuration</td>
</tr>
<tr>
<td>Copy a scan</td>
<td>Copy a Scan Configuration</td>
<td>Copy a Scan Configuration</td>
</tr>
<tr>
<td>Change scan ownership</td>
<td>Change Scan Ownership</td>
<td>Change Scan Ownership</td>
</tr>
<tr>
<td>View results for an individual scan</td>
<td>View Results for an Individual Scan</td>
<td>View Individual Scan Details</td>
</tr>
<tr>
<td>Change the scan &quot;read&quot; status</td>
<td>Change the Scan Read Status</td>
<td>Change the Scan Read Status</td>
</tr>
<tr>
<td>Export results for an individual scan</td>
<td>Export Scan Results</td>
<td>Export Scan Results</td>
</tr>
<tr>
<td>Move a scan to the trash</td>
<td>Move a Scan to the Trash Folder</td>
<td>Move a Scan to the Trash Folder</td>
</tr>
<tr>
<td>Delete a scan</td>
<td>Delete a Scan</td>
<td>Delete a Scan</td>
</tr>
<tr>
<td>Manage scan folders</td>
<td>Scan Folders</td>
<td>Scan Folders</td>
</tr>
</tbody>
</table>

**Policies / User-Defined Templates (see [Terminology Differences](#))**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Web App</th>
<th>Desktop Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a user-defined template</td>
<td>Create a Policy</td>
<td>Create a User-Defined Template</td>
</tr>
<tr>
<td>Edit a user-defined template</td>
<td>supported</td>
<td>Edit a User-Defined Template</td>
</tr>
<tr>
<td>Copy a user-defined template</td>
<td>Copy a Policy</td>
<td>Copy a User-Defined Template</td>
</tr>
</tbody>
</table>
### Export

<table>
<thead>
<tr>
<th>Task</th>
<th>Export</th>
<th>Export a Policy</th>
<th>Export a User-Defined Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export a user-defined template</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Import a user-defined template</td>
<td></td>
<td>Import a Policy</td>
<td>Import a User-Defined Template</td>
</tr>
<tr>
<td>Set permissions for a user-defined template</td>
<td></td>
<td>Set Permissions for a Policy</td>
<td>Edit a User-Defined Template</td>
</tr>
<tr>
<td>Change ownership of a user-defined template</td>
<td></td>
<td>Change Policy Ownership</td>
<td>Change User-Defined Template Ownership</td>
</tr>
<tr>
<td>Delete a user-defined template</td>
<td></td>
<td>Delete a Policy</td>
<td>Delete a User-Defined Template</td>
</tr>
</tbody>
</table>

### Target Groups

<table>
<thead>
<tr>
<th>Task</th>
<th>Target Groups</th>
<th>Target Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage target groups</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Exclusions

<table>
<thead>
<tr>
<th>Task</th>
<th>Exclusions</th>
<th>Exclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage exclusions</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Scanners / Sensors (see Terminology Differences)

<table>
<thead>
<tr>
<th>Task</th>
<th>Link a Scanner</th>
<th>Link a Sensor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link a scanner</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify scanner Permissions</td>
<td>Modify Scanner Permissions</td>
<td>Modify Sensor Permissions</td>
</tr>
<tr>
<td>Modify scanner settings</td>
<td>Modify Scanner Settings</td>
<td>Modify Sensor Settings</td>
</tr>
<tr>
<td>Manage scanner groups</td>
<td>Scanner Groups</td>
<td>Scanner Groups</td>
</tr>
</tbody>
</table>

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective
<table>
<thead>
<tr>
<th>Manage blackout windows</th>
<th>Blackout Windows</th>
<th>Blackout Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage agents</td>
<td>Agents</td>
<td>Agents</td>
</tr>
<tr>
<td>PCI/ASV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage PCI/ASV</td>
<td>PCI/ASV Scans</td>
<td>PCI/ASV Scans</td>
</tr>
<tr>
<td>Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Tenable.io instance information</td>
<td>About</td>
<td>View Information about Your Tenable.io Instance</td>
</tr>
<tr>
<td>View summary of your organization’s use of Tenable.io (including license information)</td>
<td>Health Status Work-bench</td>
<td>View Information about Your Tenable.io Instance</td>
</tr>
<tr>
<td>Manage recast and accept rules</td>
<td>Recast Rules</td>
<td>Recast/Accept Rules</td>
</tr>
<tr>
<td>Manage asset tags</td>
<td>Tags</td>
<td>Tags</td>
</tr>
<tr>
<td>Manage connectors</td>
<td>no classic interface maintained</td>
<td>Connectors Manage Connectors</td>
</tr>
<tr>
<td>Manage credentials</td>
<td>no classic interface equivalent</td>
<td>Managed Credentials</td>
</tr>
<tr>
<td>Manage access groups</td>
<td>no classic interface equivalent</td>
<td>Access Groups</td>
</tr>
<tr>
<td>Manage your user account</td>
<td>My Account</td>
<td>My Account</td>
</tr>
<tr>
<td>Generate an API key for your account</td>
<td>My Account</td>
<td>Generate an API Key</td>
</tr>
<tr>
<td>Manage other user accounts</td>
<td>Users</td>
<td>Users</td>
</tr>
<tr>
<td>Generate an API key for another user account</td>
<td>Generate an API Key</td>
<td>Generate an API Key</td>
</tr>
<tr>
<td>Manage user groups</td>
<td>Groups</td>
<td>Groups</td>
</tr>
<tr>
<td>Assets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------</td>
<td></td>
</tr>
<tr>
<td>Manage assets</td>
<td><strong>Assets</strong></td>
<td></td>
</tr>
<tr>
<td>View asset details</td>
<td>View Asset Vulnerabilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View Additional Info</td>
<td></td>
</tr>
<tr>
<td>Delete assets</td>
<td>Delete Assets</td>
<td></td>
</tr>
<tr>
<td>View deleted assets</td>
<td>View Deleted Assets</td>
<td></td>
</tr>
<tr>
<td>View asset activity</td>
<td>supported</td>
<td></td>
</tr>
<tr>
<td>Manage asset tags</td>
<td>Manage Asset Tags</td>
<td></td>
</tr>
<tr>
<td>Add a tag to an asset</td>
<td>Apply a Tag to an Asset</td>
<td></td>
</tr>
<tr>
<td>Search assets by tag</td>
<td>Filter Assets by Tag</td>
<td></td>
</tr>
<tr>
<td>Remove a tag</td>
<td>Remove a Tag from an Asset</td>
<td></td>
</tr>
<tr>
<td><strong>Vulnerabilities</strong></td>
<td><strong>Vulnerabilities by plugins</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Vulnerabilities by Asset</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>View vulnerability details</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>View plugin output</strong></td>
<td></td>
</tr>
<tr>
<td>Export vulnerability data</td>
<td>supported</td>
<td></td>
</tr>
<tr>
<td><strong>Dashboards</strong></td>
<td><strong>Export Vulnerability Data</strong></td>
<td></td>
</tr>
</tbody>
</table>

---

Dashboards
<table>
<thead>
<tr>
<th>Manage dashboards</th>
<th>Dashboards</th>
<th>Dashboards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronize classic and new dashboards</td>
<td>no classic interface equivalent</td>
<td>Dashboard Synchronization</td>
</tr>
<tr>
<td>Create a dashboard</td>
<td>Create a Dashboard</td>
<td>Create A Dashboard</td>
</tr>
<tr>
<td>Edit a dashboard</td>
<td>Configure a Dashboard</td>
<td>Edit a Dashboard</td>
</tr>
<tr>
<td>Filter a dashboard</td>
<td>Filter a Dashboard</td>
<td>Filter a Dashboard</td>
</tr>
<tr>
<td>Export a dashboard</td>
<td>Export a Dashboard</td>
<td>Export a Dashboard (PDF export only)</td>
</tr>
<tr>
<td>Customize dashboards with dashboard widgets</td>
<td>Configure a Dashboard Component</td>
<td>Configure Dashboard Widgets</td>
</tr>
<tr>
<td>Set a Default Dashboard</td>
<td>Set a Default Dashboard</td>
<td>Set a Default Dashboard</td>
</tr>
</tbody>
</table>

**Reports**

| Manage reports | Reports | Dashboards |

**Additional Resources**
Install data acquisition tools | Install Data Acquisition Tools | no change

**Tenable.io Container Security**

Scan images and containers for vulnerabilities | no classic interface maintained | Welcome

**Tenable.io Web Application Scanning**

Scan web applications for vulnerabilities | Welcome | development pending

**Terminology Differences**

The table below briefly lists terminology differences between the classic and new interfaces.

<table>
<thead>
<tr>
<th>Classic</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>scanners</td>
<td>sensors</td>
</tr>
<tr>
<td>impersonate a user</td>
<td>assist a user with their account</td>
</tr>
<tr>
<td>policy</td>
<td>template</td>
</tr>
</tbody>
</table>
Transition to the New WAS Interface

Required Additional License: Tenable.io Web Application Scanning

On March 1, 2021, Tenable activated the new interface and set the classic interface to read-only mode for all of your users. For more information, see Activate the New Interface.

Welcome to the new Tenable.io Web Application Scanning interface!

Tenable designed this new interface to improve the efficiency and ease of your workflow as you configure scans and analyze scan results.

The system requirements are the same for both classic and new interfaces.

Feature Parity

The table below lists which tasks are supported in each interface.

<table>
<thead>
<tr>
<th>Task</th>
<th>Classic</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get Started</td>
<td>Get Started with WAS</td>
<td></td>
</tr>
<tr>
<td>Get started</td>
<td>Get Started with WAS</td>
<td></td>
</tr>
<tr>
<td>Navigate</td>
<td>Navigate the Classic Interface in WAS (Classic Interface)</td>
<td>Navigate Tenable.io (New Interface)</td>
</tr>
<tr>
<td>View license information</td>
<td>no classic interface equivalent</td>
<td>View Information about Your Tenable.io Instance</td>
</tr>
<tr>
<td>Scans</td>
<td>Create a Scan (Classic Interface)</td>
<td>Create a WAS Scan</td>
</tr>
<tr>
<td>Create or edit a scan configuration</td>
<td>Create a Scan (Classic Interface)</td>
<td>Create a WAS Scan</td>
</tr>
</tbody>
</table>

Note: In the classic Tenable.io Web Application Scanning interface, the Legacy Web App Scan template appears in the Web Application tab of the Tenable-provided scan templates. In the new interface, this template appears in the Scanner tab.
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Equivalent Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create or edit a scan configuration for PCI/ASV compliance</td>
<td>Create a Scan (Classic Interface) (PCI WAS Scan template)</td>
<td>Create a WAS Scan (PCI scan template)</td>
</tr>
<tr>
<td>Create or edit an API scan configuration</td>
<td>no classic interface equivalent</td>
<td>Create a WAS Scan (API scan template)</td>
</tr>
<tr>
<td>Launch a scan</td>
<td>Start or Stop a Scan (Classic Interface)</td>
<td>Launch a Scan</td>
</tr>
<tr>
<td>Stop a scan</td>
<td>Start or Stop a Scan (Classic Interface)</td>
<td>Stop a Running Scan</td>
</tr>
<tr>
<td>Edit scan configurations</td>
<td>Configure Scan Settings (Classic Interface)</td>
<td>Edit WAS Scan Settings</td>
</tr>
<tr>
<td>Copy a scan configuration</td>
<td>Copy a Scan Configuration (Classic Interface)</td>
<td>Copy a Scan Configuration</td>
</tr>
<tr>
<td>Manage scan credentials</td>
<td>WAS Credentials (Classic Interface)</td>
<td>Credentials in WAS Scans</td>
</tr>
<tr>
<td>Change scan ownership</td>
<td>no classic interface equivalent</td>
<td>Change Scan Ownership</td>
</tr>
<tr>
<td>View scan results</td>
<td>View Scans (Classic Interface)</td>
<td>View WAS Scan Details</td>
</tr>
<tr>
<td>View scan notes</td>
<td>no classic interface equivalent</td>
<td>View Scan Notes</td>
</tr>
<tr>
<td>View plugin attachments</td>
<td>no classic interface equivalent</td>
<td>View Plugin Attachments</td>
</tr>
<tr>
<td>Move scan to a folder</td>
<td>supported</td>
<td>Move a Scan to a Scan Folder</td>
</tr>
<tr>
<td>Move a scan to the trash</td>
<td>supported</td>
<td>Move a Scan to the Trash Folder</td>
</tr>
<tr>
<td>Action</td>
<td>Link</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>Delete a scan permanently</td>
<td><strong>Delete a Scan (Classic Interface)</strong></td>
<td></td>
</tr>
<tr>
<td>Delete a scan job</td>
<td><strong>Delete Scan Job (Classic Interface)</strong></td>
<td></td>
</tr>
<tr>
<td>Import a scan</td>
<td>supported</td>
<td>development pending</td>
</tr>
<tr>
<td>Export scan results</td>
<td><strong>Export Scan Results (Classic Interface)</strong></td>
<td></td>
</tr>
<tr>
<td>View scan audit trails</td>
<td>supported</td>
<td>development pending</td>
</tr>
</tbody>
</table>

**Policies/User-Defined Scan Templates (see [Terminology Differences](#))**

<table>
<thead>
<tr>
<th>Action</th>
<th>Link</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a user-defined scan template</td>
<td>supported</td>
<td>Create a User-Defined Template</td>
</tr>
<tr>
<td>Edit a user-defined scan template</td>
<td>supported</td>
<td>Edit a User-Defined Template</td>
</tr>
<tr>
<td>Copy a user-defined scan template</td>
<td>no classic interface equivalent</td>
<td>Copy a User-Defined Template</td>
</tr>
<tr>
<td>Set permissions for a user-defined scan template</td>
<td>supported</td>
<td>Edit a User-Defined Template</td>
</tr>
<tr>
<td>Change ownership of a user-defined scan template</td>
<td>supported</td>
<td>Change User-Defined Template Ownership</td>
</tr>
<tr>
<td>Delete a user-defined scan template</td>
<td>supported</td>
<td>Delete a User-Defined Template</td>
</tr>
</tbody>
</table>

**Dashboards**

<table>
<thead>
<tr>
<th>Action</th>
<th>Link</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage dashboards</td>
<td><strong>Web Applications Workbench (Classic Interface)</strong></td>
<td></td>
</tr>
</tbody>
</table>

Dashboards
<table>
<thead>
<tr>
<th>View dashboard templates</th>
<th>no classic interface equivalent</th>
<th>View the Dashboards Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a dashboard</td>
<td>no classic interface equivalent</td>
<td>Create a Dashboard</td>
</tr>
<tr>
<td>Customize dashboards with dashboard widgets</td>
<td>no classic interface equivalent</td>
<td>Add a Widget to a Dashboard</td>
</tr>
<tr>
<td>Configure a dashboard</td>
<td>no classic interface equivalent</td>
<td>Manage Widgets</td>
</tr>
<tr>
<td>Duplicate a dashboard</td>
<td>no classic interface equivalent</td>
<td>Duplicate a Dashboard</td>
</tr>
<tr>
<td>Delete a dashboard</td>
<td>no classic interface equivalent</td>
<td>Delete a Dashboard</td>
</tr>
</tbody>
</table>

**Terminology Differences**

The table below briefly lists terminology differences between the classic and new interfaces.

<table>
<thead>
<tr>
<th>Classic Interface</th>
<th>New Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy</strong> – A set of predefined configuration options related to performing a scan. You can create a policy to share a configured template with other users.</td>
<td><strong>Scan Template</strong> – A set of predefined configuration options related to performing a scan. You can use one of the Tenable-provided scan templates to create a scan, or you can create a user-defined scan template to share a configured template with other users.</td>
</tr>
</tbody>
</table>
Activate the New Interface for WAS

On March 1, 2021, Tenable will activate the new interface and set the classic interface to read-only mode for all of your users.

Required Additional License: Tenable.io Web Application Scanning

Required User Role: Administrator

If you activate the new interface, Tenable.io Web Application Scanning operates in the read-only classic/read-write new mode.

If you activate the new interface, you activate it for all users in your organization's Tenable.io Web Application Scanning instance. You cannot activate the new interface by individual user account.

If you do not activate the new interface, all users in your organization's Tenable.io Web Application Scanning instance remain on the old interface, with read-only permissions for the new interface.

Caution: You cannot revert to the classic interface after you activate the new interface.

Before you begin:

- Review Transition to the New WAS Interface and ensure you understand the tasks you can and cannot yet complete in the new interface.

To activate the new interface for your organization's Tenable.io Web Application Scanning instance:

1. In the upper-right corner of any page, click Activate New WAS Interface.

   The Activate WAS in the new interface plane expands.

2. Select the I acknowledge that WAS will be activated in the new interface for all users on this account check box.

3. Click Confirm.

   Your default dashboard in the new interface appears.
Interface Activation Modes in WAS

Tenable.io Web Application Scanning supports the following activation modes:

- **Read-write classic/read-only new**
- **Read-only classic/read-write new**

**Read-write Classic/Read-only New**

If you have historically used the classic interface in Tenable.io Web Application Scanning, you can continue using the classic interface to create and configure scans, as well as view or export scan results. You can preview all the functionality that exists in the new interface, but you cannot perform any related tasks in the new interface.

**Read-only Classic/Read-write New**

If you activate the new interface in Tenable.io Web Application Scanning, the actions you can take depend on the Tenable-provided scan template on which a scan is based.

<table>
<thead>
<tr>
<th>Template</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI WAS Scan</td>
<td>Use the classic interface to create and modify these configurations, as well as view and export scan results. These actions are supported in the classic interface only.</td>
</tr>
<tr>
<td>Any</td>
<td>Use the new interface to do the following:</td>
</tr>
<tr>
<td></td>
<td>○ <strong>Create</strong> and <strong>modify</strong> new scan configurations.</td>
</tr>
<tr>
<td></td>
<td>○ <strong>Modify</strong> historical scan configurations.</td>
</tr>
<tr>
<td></td>
<td>○ <strong>View</strong> and <strong>export</strong> both new and historical results for any scan.</td>
</tr>
</tbody>
</table>

At the time you activate the new interface, Tenable.io Web Application Scanning creates a historical snapshot of the existing scan configurations and results. In the classic interface, you can view historical scan configurations, but the snapshot version does not reflect changes you might make to those configurations in the new interface. For historical scan configurations, you can view and export scan results in either interface.
Access the New Interface

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To access the new interface:

1. Do one of the following:
   - In the top navigation bar of the classic interface, click the New Interface button. This button does not appear on low-resolution monitors.
   - In the top navigation bar of the classic interface, click Vulnerability Management > New Interface or Web Applications > New Interface.

   When you access the new interface in Tenable.io Vulnerability Management, the default dashboard you set for the new interface appears.

2. To access other pages in the new interface, click the button in the upper-left corner of the page.
View Notifications

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

In Tenable.io, the **Notifications** panel displays a list of system notifications. The 📣 button shows the current number of unseen notifications. When you open the **Notifications** panel, Tenable.io marks those notifications as seen. Once you have seen a notification, you can clear it to remove it from the **Notifications** panel.

**Note:** Tenable.io groups similar notifications together.

To view notifications in the new interface:

1. In the upper-right corner, click the 📣 button.

   The **Notifications** panel appears and displays a list of system notifications.

   In the **Notifications** panel, you can do the following:
   - To clear one notification, next to the notification, click the ✗ button.
   - To expand a group of notifications, at the bottom of the grouped notification, click **More Notifications**.
   - To collapse an expanded group of notifications, at the top of the expanded notifications, click **Show Less**.
   - To clear an expanded group of notifications, at the top of the expanded notifications, click **Clear Group**.
   - To clear all notifications, at the bottom of the panel, click **Clear All**.
Access the User Account Menu

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To access the user account menu:

1. In the upper-right corner, click the button.
   
The user account menu appears.

2. Do one of the following:
   - Click **My Account** to make changes to your own user account. See [My Account](#) for more information.
   - Log out of Tenable.io. See [Log Out of the New Interface](#) for more information.
Access the Quick Actions Menu

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

The quick actions menu displays a list of common actions.

To access the quick actions menu:

1. In the upper-right corner, click the 🔄 **Quick Actions** button.

   The quick actions menu appears.

2. Click a link to begin one of the following actions:

   - [Create a scan](#)
   - [Add a dashboard](#)
   - [Add a recast rule](#)
   - [View all scans](#)
   - [View all vulnerabilities](#)
Access the Resource Center

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

The Resource Center displays a list of informational resources including product announcements, Tenable blog posts, and user guide documentation.

To access the Resource Center:

1. In the upper-right corner, click the button.

   The Resource Center menu appears.

2. Click a resource link to navigate to that resource.
Navigate Breadcrumbs

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

In the new interface, certain pages display breadcrumbs in the top navigation bar. From left to right, the breadcrumbs show the path of pages you visited to reach your current page:

```
=str
tenable.io® | Vulnerability Management › Vulnerabilities › Vulnerability Details › Asset Details
```

or

```
=str
tenable.io® | Web Application Scanning › Vulnerabilities › Application Details
```

To navigate breadcrumbs:

- In the top navigation bar, click a link in the breadcrumb trail to return to a previous page.
Navigate Planes

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

The new interface combines fixed pages with overlapping planes.

To navigate planes in the new interface:

1. Access a plane using one of the following methods:
   - Click a widget on a dashboard.
   - Use the left navigation plane as follows:
     a. In the upper-left corner, click the button.

     The left navigation plane appears.

     b. In the left navigation plane, click a menu option.

     With the exception of the left navigation plane, planes open from the right side of the screen.

2. Manipulate a plane using the following buttons at the left edge of the plane:

<table>
<thead>
<tr>
<th>Button</th>
<th>Short Name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>❯</td>
<td>expand</td>
<td>Expand a plane. Some planes can expand to full screen.</td>
</tr>
<tr>
<td>⏉</td>
<td>retract</td>
<td>Retract an expanded plane to its default size.</td>
</tr>
<tr>
<td>✗</td>
<td>close</td>
<td>Close a plane.</td>
</tr>
<tr>
<td>←</td>
<td>expand preview</td>
<td>Expand a preview plane.</td>
</tr>
<tr>
<td>→</td>
<td>retract preview</td>
<td>Retract an expanded plane to the preview plane.</td>
</tr>
</tbody>
</table>

3. Return to a previous plane or page (and close a new plane or planes) by clicking the previous plane.
In Tenable.io, there are two types of tables: standard tables and customizable tables.

**Standard Tables**

Standard tables in Tenable.io feature mainly navigational capabilities. You can search, filter, sort, and navigate through pages of the table. You cannot, however, adjust the column widths, column order, or add or remove columns from the table. For more information, see [Interact with a Standard Table](#).

**Customizable Tables**

Like standard tables, customizable tables feature search and navigational capabilities. They also include the ability to drag and drop columns in any order, change column width, and sort the data in multiple columns at one time. For more information, see [Interact with a Customizable Table](#).
Interact with a Standard Table

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To interact with a standard table in the new interface:

1. View a standard table.
2. Do any of the following:
   - **Navigate the table:**
     - To adjust the sort order, click a column title.
       - Tenable.io sorts all pages of the table by the data in the column you selected.
     - In Tenable.io Vulnerability Management, to increase or decrease the number of rows displayed per page, click **Results per page** and select a number.
       - Tenable.io refreshes the table.
     - In Tenable.io Vulnerability Management, to view all action buttons available in a table row, click the **button**.
       - This button appears instead of individual action buttons if 5 or more actions are possible for the row.
     - To navigate to another page of the table, click the arrows:

<table>
<thead>
<tr>
<th>Button</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>⬤</td>
<td>Navigate to the first page of the table.</td>
</tr>
<tr>
<td>⬣</td>
<td>Navigate to the previous or next page of the table.</td>
</tr>
<tr>
<td>⬦</td>
<td>Navigate to the last page of the table.</td>
</tr>
</tbody>
</table>
• **Filter** the table.

• **Search the table:**

  In the new interface, a search box typically appears above an individual table but may also appear next to the **Filters** box.

  a. In the **Search** box, type your search criteria.

     Your search criteria depends on the type of data in the table you want to search.

  b. Click the **Search** button.

     Tenable.io filters the table by your search criteria.

• **Change the table date range:**

  **Tip:** The Tenable-provided date ranges include:

  • **Last 7 Days** – A scan identified the vulnerability or asset within the last 7 days.
  • **Last 14 Days** – A scan identified the vulnerability or asset within the last 14 days.
  • **Last 30 Days** – A scan identified the vulnerability or asset within the last 30 days.
  • **Last 90 Days** – A scan identified the vulnerability or asset within the last 90 days.
  • **All** – A scan identified the vulnerability or asset at any time, including earlier than 90 days ago.

  **Note:** By default, the first time you access these pages during a Tenable.io session, the date range is set to **Last 30 Days**.

  a. In the upper-right corner of the page, next to the date range box, click the **▼** button.

     The date range list appears.

  b. Select a date range.

     Tenable.io applies the date range to the table.
Interact with a Customizable Table

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Note:** Customizable tables also include the ability to access the actions buttons by right-clicking a table row. To access your browser menu, press the Ctrl key and right-click.

To interact with a customizable table in the new interface:

1. View a customizable table.
2. Do any of the following:
   - **Navigate the table:**
     - To adjust the sort order, click a column title.
       - Tenable.io sorts all pages of the table by the data in the column you selected.
     - In Tenable.io Vulnerability Management, to increase or decrease the number of rows displayed per page, click **Results per page** and select a number.
       - Tenable.io refreshes the table.
     - To view all action buttons available in a table row, click the ☰ button.
       - This button appears instead of individual action buttons if 5 or more actions are possible for the row.
     - To navigate to another page of the table, click the arrows:

<table>
<thead>
<tr>
<th>Button</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;&lt;</td>
<td>Navigate to the first page of the table.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Navigate to the previous or next page of the table.</td>
</tr>
<tr>
<td>&gt;&gt;&gt;</td>
<td>Navigate to the last page of the table.</td>
</tr>
</tbody>
</table>

- **Search the table:**
In the new interface, a search box appears above individual tables in various pages and planes. In some cases, the search box appears next to the Filters box.

- In the Search box, type your search criteria.
  
  Your search criteria depends on the type of data in the table you want to search.

- Click the button.
  
  Tenable.io filters the table by your search criteria.

- To change the column order, drag and drop a column header to another position in the table.

- Remove or add columns:
  
  - Roll over any column.
    
    The button appears in the header.
  
  - Click the button.
    
    A column selection box appears.
  
  - Select or clear the check box for any column you want to show or hide in the table.

  **Tip:** Use the search box to quickly find a column name.

  The table updates based on your selection.

- Adjust column width:
  
  - Roll over the header between two columns until the resize cursor appears.
  
  Click and drag the column width to the desired width.

  **Tip:** To automatically resize a column to the width of its content, double-click the right side of the column header.

- To sort data in the table, click a column header.
  
  Tenable.io sorts all pages of the table by the data in the column you selected.
• To sort data in the table by multiple columns, press **Shift** and click one or more column headers.

**Note:** Not all tables or columns support sorting by multiple columns.

Tenable.io sorts all pages of the table in the order in which you selected the columns.
Filter a Table

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

In the new interface, a **Filters** box appears above individual tables in various pages and planes.

To filter a table in the new interface:

1. Next to **Filters**, click the ▼ button.
   The filter settings appear.

2. In the **Match** drop-down box, select one of the following:
   - **Match Any** – View results that match any of the filters you create.
   - **Match All** – View results that match all of the filters you create.

3. (Optional) In Tenable.io Vulnerability Management, to quick-select filters, click ⭐ **Select Filters**.
   A drop-down list appears.
   - a. In the drop-down list, search for the filter you want to apply.
      The list updates based on your search criteria.
   - b. Select the check box next to the filter or filters you want to apply.
      The selected filters appear in the filter section.

4. In the **Select Category** drop-down box, select an attribute.
   For example, in Tenable.io Vulnerability Management, you might select **Severity** if filtering vulnerabilities or **Asset ID** if filtering assets.
5. In the **Select Operator** drop-down box, select an operator.

**Note:** When using the **contains** or **does not contain** operators, use the following best practices:

- For the most accurate and complete search results, use full words in your search value.
- Do not use periods in your search value.
- Remember that when filtering **assets**, the search values are case sensitive.
- Where applicable, Tenable recommends using the **contains** or **does not contain** instead of the **is equal to** or **is not equal to** operators.

6. In the **Select Value** box, do one of the following:

<table>
<thead>
<tr>
<th>Value Type</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text</td>
<td>Type the value on which you want to filter.</td>
</tr>
<tr>
<td></td>
<td>An example of the expected input is present in the box until you start typing. If what you type is invalid for the attribute, a red outline appears around the text box.</td>
</tr>
<tr>
<td>Single valid value</td>
<td>If a default value is associated with the attribute, Tenable.io selects the default value automatically.</td>
</tr>
<tr>
<td></td>
<td>To change the default value, or if there is not an associated default value present:</td>
</tr>
<tr>
<td></td>
<td>a. Click the box to display the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>b. Search for and select one of the listed values.</td>
</tr>
<tr>
<td>Multiple valid values</td>
<td>To select one or more values:</td>
</tr>
<tr>
<td></td>
<td>a. Click the box to display the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>b. Search for and select a value.</td>
</tr>
<tr>
<td></td>
<td>The selected value appears in the box.</td>
</tr>
</tbody>
</table>
c. Repeat until you have selected all appropriate values

d. Click outside the drop-down list to close it.

To deselect values:

a. Roll over the value you want to remove.
   The \( \times \) button appears over the value.

b. Click the \( \times \) button.
   The value disappears from the box.

7. (Optional) In the lower-left corner of the filter section:
   - To add another filter, click the **Add** button.
   - To clear all filters, click the **Reset Filters** button.

8. Click **Apply**.

   Tenable.io applies your filter or filters to the table.

9. (Optional) In Tenable.io Vulnerability Management, **save** your filter or filters for later use.

10. (Optional) **Clear** the filters you applied.
Clear Table Filters

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To clear filters from a table in the new interface:

1. View a table where you previously applied one or more filters.
   
   For example, view the plugins table in the Vulnerabilities page.

2. In the table header, click **Clear All Filters**.
   
   Tenable.io clears all filters from the table, including saved searches.

   **Note:** Clearing filters does not change the date range selected in the upper-right corner of the page. For more information, see Tenable.io Tables.
Saved Search

Some analysis pages feature the ability to filter table data. For example, while viewing the By Plugin tab of the Vulnerabilities page, you can use vulnerability filters to limit the data in the plugins table. The Saved Search feature allows you to save frequently used filter parameters. You can then easily access the saved search for future use, or share the search with other members of your team.

Saved searches are specific to the analysis page where you create them. For example, a saved search created on the Vulnerabilities page cannot be used in the Assets page.

For more information, see:
Create a Saved Search

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To create a saved search:

1. **Add** a filter or filters to create the search that you want to save.
2. In the upper-right table header, click the button.

   A text box appears.

3. Type a unique name for the search.
4. Click the button to save the search.

   The text box closes. The newly-saved search appears in the saved search drop-down box.

What to do next:

- **Apply** the saved search at a later time.
- (Optional) **Share** the saved search with other users in your organization.
Edit a Saved Search

Required Tenable.io Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Tenable.io Web Application Scanning User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

To edit the name of a saved search:

1. In the upper-right table header, select the saved search you want to edit from the Saved Search drop-down menu.
2. Next to the button, click the button.

   A list of options appears.
3. Click Edit.

   The text box for the saved search's name becomes editable.
4. Modify the text.
5. Click the button.

   The editable text box closes. Tenable.io updates the saved search.

To edit the parameters of a saved search:

1. In the upper-right table header, select the saved search you want to edit from the Saved Search drop-down menu.
2. Add, edit, or delete a filter.
3. Click Apply.

   Tenable.io detects the changed search parameters and prompts you to select one of the following options:
<table>
<thead>
<tr>
<th>Update</th>
<th>Applies the change(s) to the existing saved search.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t Update</td>
<td>Applies the filter to the current view, but does not apply it to the saved search.</td>
</tr>
<tr>
<td>Save as New</td>
<td>Creates a new saved search that includes the applied updates.</td>
</tr>
</tbody>
</table>

4. Click **Update** to save the changes you made.
Apply a Saved Search

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To apply a saved search:

1. View the table where you want to apply the saved search.
   
   For example, view the plugins table on the Vulnerabilities page.

2. In the upper-right corner of the space above the table, click the ▼ button next to the Saved Search drop-down box.

   **Note:** The Saved Search drop-down box only appears if you have previously created a saved search or another user has shared a saved search with you.

3. In the drop-down list, select the saved search you want to apply.

4. (Optional) **Clear** the saved search.
Share a Saved Search

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To share a saved search:

1. In the upper-right table header, select the saved search you want to edit from the Saved Search drop-down menu.
2. Next to the button, click the button.
   A list of options appears.
3. Click Share.
   The Shared Search plane appears.
4. Click the Search by user or group name box.
5. Enter a recipient or select from the list of pre-configured users.
6. Click Share.
   A confirmation message appears.
Delete a Saved Search

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To delete a saved search:

1. In the upper-right table header, select the saved search you want to edit from the Saved Search drop-down menu.
2. Next to the button, click the button.
   
   A list of options appears.
3. Click **Delete**.
   
   A confirmation message appears.
4. Click **Delete**.
   
   Tenable.io deletes the saved search.
Return to the Classic Interface

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To return to the classic interface from the new interface:

1. In the upper-left corner, click the button.
   
The left navigation plane appears.

2. In the left navigation plane, click **Classic Interface**.
   
   Your default dashboard in the classic interface appears.

   **Note:** In the left navigation plane, if you click **Scans**, Tenable.io jumps you directly to the related pages in the classic interface.
Log Out of the New Interface

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To log out of the new interface:

1. In the upper-right corner, click the button.

   The user account menu appears.

2. Click **Sign Out**.
Navigate Tenable.io (Classic Interface)

Tip: This topic describes navigation in the classic Tenable.io. For information about the new interface, see Navigate Tenable.io (New Interface).

The top navigation bar displays a toggle to switch between Tenable.io Vulnerability Management, Tenable.io Container Security, and Web Applications, as well as links to the four main pages: Dashboards, Scans, Reports, and Settings. All of the Tenable.io Vulnerability Management primary tasks can be performed using these four pages. Click a page name to open the corresponding page.

On the right side of the top navigation bar, you can find the following options:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced</td>
<td>Displays the Advanced Search box. See the Search documentation for more information about advanced search.</td>
</tr>
<tr>
<td>Search</td>
<td>Searches the current page. See the Search documentation for more information about contextual search.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The Search box does not appear on every page.</td>
</tr>
<tr>
<td>Help</td>
<td>Toggles the Need Help? box, which displays a list of common Tenable.io tasks. Click a link to begin a walkthrough guide.</td>
</tr>
<tr>
<td>Notifications</td>
<td>Toggles the Notifications box, which displays a list of notifications, successful or unsuccessful login attempts, errors, and system information generated by Tenable.io.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Notifications are not preserved between sessions. Unread notifications are removed from the list when the user logs out.</td>
</tr>
<tr>
<td>Username</td>
<td>Displays a drop-down menu with the following options: My Account, What's New, Documentation, and Sign Out.</td>
</tr>
</tbody>
</table>
Search (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

On the top navigation bar, a search box appears on most pages in Tenable.io. The search box is contextual, and provides different results based on the page currently in view. For example, on the Vulnerabilities dashboard, you can use the search box to filter the table of plugins that appears at the bottom of the page. If a page does not support searching, the search box does not appear on the top navigation bar.

Additionally, some pages support advanced searching.

To access the advanced search options:

1. On the top navigation bar, click the **Advanced** link.

   The **Advanced Search** window appears.

The exact options available on the **Advanced Search** window vary based on the page currently in view. Generally, advanced searching allows you to filter the information on the page based on factors that you specify. If a page does not support advanced searching, the **Advanced** link does not appear on the top navigation bar.
Navigate the Classic Interface in WAS (Classic Interface)

On March 1, 2021, Tenable activated the new interface and set the classic interface to read-only mode for all of your users. For more information, see Activate the New Interface.

Tip: This topic describes navigation in the Tenable.io Web Application Scanning classic interface. For information about the new interface, see Navigate Web Application Scanning in the New Interface.

The top navigation bar displays a toggle to switch between the Tenable.io products (Vulnerability Management, Container Security, and Web Applications), as well as links to the four main pages: Dashboards, Scans, Reports, and Settings. You can perform all Tenable.io primary tasks using these four pages. Click a page name to open the corresponding page.

On the right side of the top navigation bar, you can find the following options:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟍</td>
<td>Toggles the Need Help? box, which displays a list of common Tenable.io tasks. Click a link to begin a walkthrough guide.</td>
</tr>
<tr>
<td>📣</td>
<td>Toggles the Notifications box, which displays a list of notifications, successful or unsuccessful login attempts, errors, and system information generated by Tenable.io. Note: Notifications are not preserved after a session expires.</td>
</tr>
<tr>
<td>Username</td>
<td>Displays a drop-down menu with the following options: My Account, What's New, Documentation, and Sign Out.</td>
</tr>
</tbody>
</table>

To access the Tenable.io Web Application Scanning workbench:

1. In Tenable.io, in the top navigation bar, click Dashboards. The Vulnerabilities workbench appears.

2. In the left navigation bar, click Web Applications.
The **Web Applications** workbench appears.

To access the Tenable.io Web Application Scanning scan templates:

1. In Tenable.io, in the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the upper right corner, click the **New Scan** button.
   
   The **Scan Templates** page appears.

3. Click the **Web Application** tab.
The Web Application scan templates appear.

<table>
<thead>
<tr>
<th>Web App Overview</th>
<th>Web App Scan</th>
<th>Legacy Web App Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>A scan that outlines URL paths and builds a site map.</td>
<td>A scan that checks a web application for vulnerabilities.</td>
<td>Configure a scan using Nessus Scanner.</td>
</tr>
</tbody>
</table>
You can create, configure, and manage scans in Tenable.io.

<table>
<thead>
<tr>
<th>Section</th>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Management Scanning Overview</td>
<td>New or Classic</td>
<td>Get started with Vulnerability Management scans.</td>
</tr>
<tr>
<td>Web Application Scanning Overview</td>
<td>New</td>
<td>Get started with web application scans.</td>
</tr>
<tr>
<td>Manage Scans</td>
<td>New or Classic</td>
<td>Create, import, and launch scans. View and manage scans and scan results.</td>
</tr>
<tr>
<td>Scan Templates and Settings</td>
<td>New or Classic</td>
<td>Use a Tenable-provided scanner template, agent template or a user-defined template to configure scan settings.</td>
</tr>
<tr>
<td>Target Groups</td>
<td>New or Classic</td>
<td>Create and manage target groups to set permissions on which hosts a user can scan.</td>
</tr>
<tr>
<td>Exclusions</td>
<td>New or Classic</td>
<td>Create and manage exclusions to restrict the scanning of specific hosts based on a selected schedule.</td>
</tr>
<tr>
<td>Scanners</td>
<td>Classic</td>
<td>Link your scanners to Tenable.io.</td>
</tr>
</tbody>
</table>

**Note:** This section describes the new interface. For information about the classic interface, see [Scans (Classic Interface)](#). For information about navigating the new interface, see [Navigate Tenable.io (New Interface)](#).
<table>
<thead>
<tr>
<th>Agents</th>
<th>Classic</th>
<th>Link your agents to Tenable.io.</th>
</tr>
</thead>
</table>

**Note:** For agents in the new interface, see [Agents](#).
Vulnerability Management Scanning Overview

Configure scans to collect data for Tenable.io. This overview walks you through the main steps you need to create, configure, launch, and manage scans.

Depending on your organization, one person may perform all of the steps, or several people may share the steps.

**Note:** Tenable recommends that you limit the number of individual scans on your network. For example, you can re-use scheduled scans instead of creating new scans. This approach can help you to avoid latency issues in the user interface.

**Note:** PCI Quarterly External scan data is intentionally excluded from dashboards, reports, and workbenches. This is due to the scan's paranoid nature, which may lead to false positives that would otherwise not be detected. For more information, see [PCI ASV Scanning Overview](#).

Create and launch an assessment scan

1. [Create a scan](#).
2. Select a scan template that fits your needs.
   - Use a [Tenable-provided scanner template](#).
   - Use a [Tenable-provided Agent template](#).
   - Create and use a [user-defined template](#).
3. Configure the scan:
   - Configure the [scan settings](#) available for your template.
     
     For information about scan targets, see [Scan Targets](#).
   - (Optional) To run a credentialed scan, configure [credentials](#).
   - (Optional) To run a compliance scan, select the [compliance audits](#) your scan includes.
   - (Optional) If you are using an advanced scan template, select what [plugins](#) your scan includes.
4. [Launch the scan](#).
View and manage scans

1. View your configured scans.
   - View scan details and scan results for a specific scan.
   - Manage scan folders.

2. To analyze data across all your scan results, see Analysis.

Refine scanning settings

- Use exclusions to restrict the scanning of specific hosts based on a selected schedule.
- Use target groups to set permissions on which hosts a user can scan.
- To understand scan distribution concepts such as scanner capacity, job queues, and how Tenable.io dispatches tasks, see Scan Distribution.
## Discovery Scans vs. Assessment Scans

You can perform two types of scans using Tenable products: *discovery scans* and *assessment scans*. Tenable recommends performing discovery scans to get an accurate picture of the assets on your network and assessment scans to understand the vulnerabilities on your assets.

For information about how discovered and assessed assets are counted towards your license, see [Tenable.io Vulnerability Management Licenses](#).

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Licensing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery scans</td>
<td>Find assets on your network.</td>
<td>Assets identified by discovery scans do not count toward your license.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• a scan configured with the Host Discovery template.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• a scan configured to use only discovery plugins.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• a scan configured to use NNM in discovery mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Video:</strong> <a href="#">Launch a Discovery Scan in Tenable.io</a></td>
<td></td>
</tr>
<tr>
<td>Assessment scans</td>
<td>Find vulnerabilities on your assets.</td>
<td>In general, assets assessed by assessment scans count toward your license.</td>
</tr>
<tr>
<td></td>
<td>For example, run an authenticated or unauthenticated scan using a Nessus scanner or Nessus Agent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Authenticated Scans</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configure authenticated scans, also known as credentialed scans, by adding access credentials to your assessment scan configuration.</td>
<td></td>
</tr>
</tbody>
</table>
Credentialed scans can perform a wider variety of checks than non-credentialed scans, which can result in more accurate scan results. This facilitates scanning of a very large network to determine local exposures or compliance violations.

Credentialed scans can perform any operation that a local user can perform. The level of scanning depends on the privileges granted to the user account. The more privileges the scanner has via the login account (e.g., root or administrator access), the more thorough the scan results.

For more information, see Credentials (Classic Interface).

**Video:** [Launch a Credentialed Scan in Tenable.io](#)

### Unauthenticated Scans

If you do not add access credentials to your assessment scan configuration, Tenable.io performs a limited number of checks when scanning your assets.
Example: Identify Assets That Have Not Been Assessed

Video: Measuring Scan Coverage in Tenable.io

Tenable.io can discover, or see, assets without assessing the assets for vulnerabilities (for example, via a host discovery scan, Nessus Network Monitor running in discovery mode, or connectors). Assets that have been seen but not assessed do not count towards your asset license limit. For a list of conditions that cause an asset to be assessed, see How Assets are Counted. However, once assessed, the asset is always categorized as assessed, even if it ages out of the license count.

This licensing exception allows you to discover assets on your network without the large number of assets counting towards your license limit. After you discover your assets, you can then identify which assets have not yet been assessed for vulnerabilities, and choose which of those assets you want to scan and manage going forward.

To identify assets that have not been assessed:

1. Discover assets using any of the following methods:
   a. Create and launch a host discovery scan in Tenable.io.
   b. Configure Nessus Network Monitor with discovery mode enabled, linked to Tenable.io.
   c. Configure a connector.

   Assets discovered by these methods do not count towards your asset license limit until they have been assessed for vulnerabilities.

2. Filter for assets that have not been assessed.
   a. In the assets table, create a filter with the following settings:
      a. In the Category box, select Asset Assessed.
      b. In the Operator box, select is equal to.
      c. In the Value box, select false.
   a. Click Apply.

   Tenable.io filters for assets that have not yet been assessed for vulnerabilities.

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable,Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective
Note: Unassessed assets (where Asset Assessed is equal to false) can differ from unlicensed assets (where Is Licensed (VM) is equal to false). Once you scan an asset for vulnerabilities, Tenable.io categorizes the asset as assessed from that point on, but the licensing status of an asset can change over time as assets are deleted or age out of your organization’s license count.

b. (Optional) Save the search for later use.

3. (Optional) Tag assets to identify assets that have not been assessed.
   a. Create manual or automatic tags to identify assets that have not been assessed.
      For example, Assets:NotYetAssessed.
   b. Manually apply the tag to assets, or create tag rules that automatically filter for assets that have not been assessed.
      For example, to create a dynamic tag for assets that have not yet been assessed, set the tag rules to filter for Asset Assessed is equal to false.

4. (Optional) Create a scan to target assets using the tag you created.
   For more information, see Example: Tag-Based Scanning.
Example: Tag-Based Scanning

You can configure scans to target assets based on one or more tags you have assigned to the assets. For example, you might want to run more frequent scans of assets running a Windows operating system. Rather than manually configuring a scan to target a static group of Windows assets, you can configure Tenable.io to automatically apply a tag to any asset that a scan identifies as running Windows. Then, you can configure a scan to evaluate any asset with that tag on an appropriate frequency.

Depending on scan findings, an asset record can contain multiple identifiers—that is, multiple IPv4 addresses, IPv6 addresses, and full-qualified domain names (FQDNs). When you configure a scan to target assets based on tags, Tenable.io examines the identifiers associated with the asset in order to resolve multiple possible identifiers to a single target. For more information, see How Tenable.io Resolves Asset Tags to Targets for Scanning.

To scan assets based on tags:

1. Review the configuration guidelines and limitations for tag-based scans.
2. Create and launch a discovery scan on the network assets where you want to target the tag-based scan.
3. Create manual or automatic tags that reflect your business context.
4. Assign tags to assets manually or automatically via tag rules.
5. Create a scan and select Tags to target all assets to which any of the tags apply.

Configuration Guidelines

When configuring tag-based scans, observe the following guidelines:

- Keep the number of assets included in a single tag-based scan as small as possible to improve performance. To do so, make the criteria for applying tags as specific as you can. For example, rather than automatically apply a tag based on multiple operating systems you want
to monitor (for example, Windows, Linux, and Mac), apply the tag based on a single operating system (for example, Windows). You can also combine multiple tags in a single scan to refine the asset list.

- Tag-based scans can target only assets that have already been identified in at least one previous scan (for example, a discovery scan), because asset identifiers must be present for assets to be evaluated for inclusion in the scan.

- When you run a Nessus scan, Tenable.io notes the FQDN or IP address that was used to scan an asset. Tenable.io uses this last-scanned FQDN or IP address for efficient lookup when re-scanning assets. Tenable recommends that you run regular discovery scans to keep the attribute updated in your asset records.

- You can configure a single scan to use tag-based targets in combination with custom targets and target groups. Tenable.io combines all targets (tag-based, custom, or target-grouped) into a single target list, then de-duplicates the targets before sending the list to the scanner.

- The scanner only scans a target if the user running the scan has Can Scan permissions for that target in an access group. To align your access group configuration with your tag-based scan configuration, do one of the following:
  - In the All Assets access group, assign Can Scan permissions to any users who might run the tag-based scan. This configuration is appropriate if your scan is based on manually-assigned tags or dynamically-assigned tags where additional access control is not required.
  - In a Manage Assets access group, configure rules that mirror the dynamic tag rules, so that the access group and the tag match the same group of assets. For example, if the tag rule matches assets where the Operating System is Windows, add access group rules that match assets where the Operating System is Windows. Then, assign any users who might run the tag-based scan Can Scan permissions in that access group. This configuration is appropriate for scans based on dynamically-assigned tags only.

Configuration Limitations

When configuring tag-based scans, keep in mind the following limitations:
• You cannot configure agent scans based on asset tags.

• You cannot use any of the following scan templates when configuring a tag-based scan: Audit Cloud Infrastructure, MDM Config Audit, Mobile Device Scan, or Offline Config Audit.

• You cannot configure tag-based scans for use by pre-authorized scanners in the AWS Marketplace. However, you can configure tag-based scans for BYOL scanners in the AWS Marketplace.

How Tenable.io Resolves Asset Tags to Targets for Scanning

To resolve a tag to a scan target, Tenable.io does the following:

1. Tenable.io matches a tag that you set in the scan to any asset where that tag is applied.

2. For each matching asset record, Tenable.io determines whether the asset was previously scanned by Nessus and has the last-scanned FQDN or IP address noted.
   • If Tenable.io can identify the asset's last-scanned FQDN or IP address, Tenable.io uses that as the target for the tag-based scan.
   • If Tenable.io is unable to determine the asset's last-scanned FQDN or IP address, Tenable.io determines which asset identifiers are present in the record. Asset identifiers include FQDN, IPv4 address, or IPv6 address. Depending on scan findings, an asset record can contain multiple identifiers.

3. If multiple identifiers are present in the asset record, Tenable.io evaluates the identifiers in the following order to determine a single target:
   • If one or more FQDNs are present, the scan target is the FQDN most recently added to the record.
   • If no FQDNs are present, and one or more IPv4 addresses are present, the scan target is the IPv4 address most recently added to the record.
   • If no FQDNs or IPv4 addresses are present, and one or more IPv6 addresses are present, the scan target is the IPv6 address most recently added to the record.

Note: When evaluating IPv4 and IPv6 addresses, Tenable.io excludes any local or broadcast addresses from consideration.
Example: Scan Routing

With *scan routing*, you can automatically dispatch scanning across multiple *scanner groups* according to the network areas to which each group has access. Scan routing reduces scan configuration and management overhead by eliminating the need to configure specific scanners for each individual scan. This feature can represent a significant benefit in large deployments. To improve operational efficiency, team members with higher privileges can manage the scanner pools, which can then be used by lower-privileged team members during scan configuration.

**Note:** Scan routing is available for *linked scanners* only.

If you configure scan routing for a scan, when the scan runs, Tenable.io automatically does the following:

- Assigns the scan targets to the scanner group configured with the narrowest matching target range.
- Within that scanner group, assigns targets to scanners as they check in, according to their capacity and the targets still available.

For more information, see [Configuration Guidelines](#).

**Note:** Tenable recommends pre-planning your scan routing strategy to efficiently target discrete areas of your network. If configured improperly, scan routing can prevent scanners from reaching their targets.

To configure scan routing:

1. Review the [configuration guidelines](#) for scan routing.
2. Configure a scanner group for scan routing.
   a. [Create](#) or [edit](#) a scanner group.
   b. In the [Targets for Scan Routing](#) box, type a comma-separated list of scan routing targets.

Targets in the list must be in the [supported formats](#).

**Note:** You can specify up to 10,000 individual scan routing targets for an individual scanner group. For example, 192.168.0.1, example.com, *.example.net, 192.168.0.0/24.
specifies four scan routing targets. To condense a scan routing target list, Tenable recommends using wildcard and range formats, instead of individual IP addresses.

c. Click **Save**.

Tenable.io saves your changes to the scanner group.

3. Configure a scan for scan routing.

   a. **Create** or **edit** a scan configuration.

   b. In the **Basic** settings section, configure the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scanner</strong></td>
<td>Select the <strong>Auto-Select</strong> option.</td>
</tr>
<tr>
<td></td>
<td>When you select this option, the <strong>Network</strong> box appears.</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• If your scans involve separate environments with overlapping IP ranges, select the <strong>network</strong> that contains the scanner groups that you configured for scan routing.</td>
</tr>
<tr>
<td></td>
<td>• If your scans do not involve separate environments with overlapping IP ranges, retain the <strong>Default</strong> network.</td>
</tr>
<tr>
<td><strong>Targets / Upload Targets / Tags</strong></td>
<td>Specify targets for the scan, using one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• In the <strong>Targets</strong> box, type the list of targets.</td>
</tr>
<tr>
<td></td>
<td>• In the <strong>Upload Targets</strong> box, upload a file of targets.</td>
</tr>
<tr>
<td></td>
<td>• In the <strong>Tags</strong> box, specify targets by tag. For more information, see Example: Tag-Based Scanning.</td>
</tr>
</tbody>
</table>

When specifying scan targets, note the following:

• Be sure to match scan targets to the scan routing targets you specify in your scanner groups.
If you specify scan targets outside the range of scanner group targets, Tenable.io scans only those hosts inside the scanner group range and returns the partial results with a warning that lists the hosts that were not scanned.

- When matching scan routing targets to scan targets, Tenable.io does not resolve FQDNs to IP addresses.

For example, if you specify *.example.com as a scan routing target, Tenable.io can assign a scan to that scanner group if the scan is configured with the scan target www.example.com. However, Tenable.io does not assign a scan to that scanner group if a scan is configured with the target 192.168.0.1, even if www.example.com could potentially resolve to 192.168.0.1.

c. Click **Save**.

Tenable.io saves your changes to the scan configuration.

**Configuration Guidelines**

- When configuring scan routes, Tenable recommends using IP ranges and CIDR ranges instead of individual IP addresses where possible. This approach differs from the recommended approach for scan targets, where narrower target values are recommended.

- Tenable.io does not support a numeric range format for IPv6 addresses. Instead, use a CIDR format for IPv6 address ranges.

- Typically, Tenable recommends adding an individual scanner to only one scanner group. In some cases, however, you may want to configure overlapping scanner groups to ensure scanning coverage or redundancy. Two or more scan groups are redundant if they target the same area of your organization's network. If Tenable.io executes a scan with redundant scanner groups, it attempts the scan using the narrowest, most-specific scanner group exclusively.

For example, two scanner groups might specify the following scan routing targets:
• Scanner Group #1 - 192.168.0.1-192.168.0.200
• Scanner Group #2 - 192.168.0.10-192.168.0.20

If your scan specifies a scan target of 192.168.0.15-192.168.0.19, Tenable.io assigns the scan to Scanner Group #2, because that group's scan routing target range is narrower than the range specified in Scanner Group #1.

• For a definition of scanner availability in a scanner group, see Scanner Groups.

Supported Scan Routing Target Formats

Tenable.io supports the following formats for scan routing targets:

<table>
<thead>
<tr>
<th>Target Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>A single IPv4 address</td>
<td>192.168.0.1</td>
</tr>
<tr>
<td>A single IPv6 address</td>
<td>2001:db8::2120:1ff:fe56:333b</td>
</tr>
<tr>
<td>An IPv4 range with a start and end address</td>
<td>192.168.0.1-192.168.0.255</td>
</tr>
<tr>
<td>An IPv4 subnet with CIDR notation</td>
<td>192.168.0.0/24</td>
</tr>
<tr>
<td>An IPv6 subnet with CIDR notation</td>
<td>2001:db8::/32</td>
</tr>
<tr>
<td>A host resolvable to either an IPv4 or an IPv6 address</td>
<td><a href="http://www.yourdomain.com">www.yourdomain.com</a></td>
</tr>
<tr>
<td>A host resolvable to either an IPv4 address or an IPv6 address</td>
<td>*.yourdomain.com</td>
</tr>
<tr>
<td>address with a wildcard as the subdomain</td>
<td></td>
</tr>
</tbody>
</table>
# Scan Status

In Tenable.io, depending on its state, scans can have following status values:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aborted</td>
<td>Either the latest run of the scan is incomplete because Tenable.io or the scanner encountered problems during the run, or the scan remained queued without running for four or more hours. For more information about the problems encountered during the run, view the scan warnings.</td>
</tr>
<tr>
<td>Canceled</td>
<td>At user request, Tenable.io successfully stopped the latest run of the scan.</td>
</tr>
<tr>
<td>Completed</td>
<td>The latest run of the scan is complete.</td>
</tr>
<tr>
<td>Empty</td>
<td>The scan is either empty (the scan is new or has yet to run) or pending (Tenable.io is processing a request to run the scan).</td>
</tr>
<tr>
<td>Imported</td>
<td>A user imported the scan. You cannot run imported scans. Scan history is unavailable for imported scans.</td>
</tr>
<tr>
<td>Pausing</td>
<td>A user paused the scan, and Tenable.io is processing the action.</td>
</tr>
<tr>
<td>Paused</td>
<td>At user request, Tenable.io successfully paused active tasks related to the scan. The paused tasks continue to fill the task capacity of the scanner that the tasks were assigned to. Tenable.io does not dispatch new tasks from a paused scan job. If the scan remains in a paused state for more than 14 days, the scan times out. Tenable.io then aborts the related tasks on the scanner and categorizes the scan as aborted.</td>
</tr>
<tr>
<td>Processing</td>
<td>Tenable.io is processing tasks for the scan. For example, Tenable.io may be importing scan results from the scanner that performed the latest run of the scan.</td>
</tr>
<tr>
<td>Resuming</td>
<td>Tenable.io is in the process of restarting tasks after the user resumed the scan. Tenable.io instructs the scanner to start the tasks from the point at which the scan was paused. If Tenable.io or the scanner encounters problems when resuming the scan, the scan fails, and Tenable.io updates the</td>
</tr>
<tr>
<td>Status</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>scan</td>
<td>The scanner did not complete the scan's latest scan job. Tenable.io Web Application Scanning may abort a scan job because the job was queued without running for more than four hours, or because Tenable.io Web Application Scanning, or the scanner, encountered other problems and aborted the scan. For more information about why Tenable.io Web Application Scanning aborted a scan, view the scan notes.</td>
</tr>
<tr>
<td>Canceled</td>
<td>At the user's request, Tenable.io Web Application Scanning successfully stopped the latest scan job.</td>
</tr>
<tr>
<td>Completed</td>
<td>The scanner completed the scan's latest scan job.</td>
</tr>
<tr>
<td>Never Run</td>
<td>The scan is either empty (the scan is new or has yet to run) or pending (Tenable.io Web Application Scanning is processing a request to run the scan).</td>
</tr>
<tr>
<td>Processing</td>
<td>The scan has completed but the results are still being processed. The scanner is processing vulnerability findings, attachments, notes, and other metadata.</td>
</tr>
<tr>
<td>Running</td>
<td>The scanner is currently running the scan.</td>
</tr>
<tr>
<td>Status</td>
<td>Description</td>
</tr>
<tr>
<td>scan</td>
<td>The scan is currently running.</td>
</tr>
<tr>
<td>Stopping</td>
<td>A user stopped the scan, and Tenable.io is processing the action.</td>
</tr>
</tbody>
</table>

**Web Application Scans**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scan</td>
<td>The scanner did not complete the scan's latest scan job. Tenable.io Web Application Scanning may abort a scan job because the job was queued without running for more than four hours, or because Tenable.io Web Application Scanning, or the scanner, encountered other problems and aborted the scan. For more information about why Tenable.io Web Application Scanning aborted a scan, view the scan notes.</td>
</tr>
<tr>
<td>Canceled</td>
<td>At the user's request, Tenable.io Web Application Scanning successfully stopped the latest scan job.</td>
</tr>
<tr>
<td>Completed</td>
<td>The scanner completed the scan's latest scan job.</td>
</tr>
<tr>
<td>Never Run</td>
<td>The scan is either empty (the scan is new or has yet to run) or pending (Tenable.io Web Application Scanning is processing a request to run the scan).</td>
</tr>
<tr>
<td>Processing</td>
<td>The scan has completed but the results are still being processed. The scanner is processing vulnerability findings, attachments, notes, and other metadata.</td>
</tr>
<tr>
<td>Running</td>
<td>The scanner is currently running the scan.</td>
</tr>
</tbody>
</table>

**Note:** Tenable.io Web Application Scanning aborts scans that remain in pending status for more than four hours. If Tenable.io Web Application Scanning aborts your scan, modify your scan schedules to reduce the number of overlapping scans. If you still have issues, contact Tenable Support.
<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stopping</td>
<td>The scanner acknowledged the <strong>stop</strong> request and is in the process of stopping.</td>
</tr>
</tbody>
</table>
Scan Distribution

Overview

The scan distribution feature improves the efficiency of scanning both for your organization’s scanners as well as the cloud scanners provided by Tenable.io for the platform as a whole. In the case of the scanners that belong to your organization, Tenable.io distributes scans as tasks across multiple scanners in the scanner group assigned to the scan, rather than assigning complete scan jobs to individual scanners. Similarly, Tenable.io distributes scans utilizing Tenable-provided cloud scanners as jobs across groups of scanners. Tenable.io breaks those jobs down into tasks and funnels them down to scanners within the groups.

In both cases, this effectively allows multiple scans to run simultaneously, eliminating bottlenecks that might otherwise occur if scans were staggered one after another on individual scanners. As the requirements of your organization grow, scan performance is less likely to degrade. Even when scans are assigned to a specific scanner, those scans are broken down into tasks that can be run simultaneously, allowing the scanner to complete the scan job more efficiently.

As scanners complete the tasks, Tenable.io immediately reflects the results. The results that were already obtained are not lost if the scan is canceled. If a scanner crashes during the scan, or a problem is encountered with a target, the other tasks run as normal.

How the Scan Distribution Feature Works

When scan jobs are created, the jobs are placed either directly in the job queue of a scanner (if that scanner was specified in the scan), or into the job queue of a scanner group.

Interacting with Scans

Because of the way the scan distribution feature breaks down scans into tasks that can be completed asynchronously, there is some nuance to the way you can interact with scans.

Scanner Groups

You can create scanner groups in order to take advantage of the scan distribution feature with your organization’s scanners. Scanner groups maximize the efficiency of your scans by spreading out
tasks across the individual scanners you assign to the group, rather than dedicating a single scanner to complete a whole job.

Scan Results

You can view scan results live, as scanners complete tasks. Each time a task completes, Tenable.io updates scan results with new data. If a scan fails or is interrupted, Tenable.io retains the already completed results, though the scan reflects that the process was not completed.

If a job is assigned to multiple scanners and one of those scanners happens to fail, the tasks dispatched to the other scanners will still be completed.
Scanner Capacity

Tenable.io considers the following three types of scanner capacities when distributing scans, in order to efficiently determine how many tasks a scanner can process.

- **Target Capacity**: The number of assets a scanner can actively scan simultaneously. This value is by default based on the hardware resources of the scanner, including the number of processors and the amount of memory available.

- **Task Capacity**: The number of tasks (parts of a scan) that a scanner can perform simultaneously. A scanner's task capacity is determined based on the target capacity.

- **Job Capacity**: The number of different jobs a scanner can include tasks from at once. In this way, scans can be performed asynchronously, and a scanner that has available capacity can complete multiple tasks even if those tasks are not derived from the same scan. Job capacity is always determined to be less than equal to the task capacity so that when a scanner is at its job capacity, it will be able to complete tasks from every job.

Scanner Group Capacity

Tenable.io also considers scanner group job capacities when distributing scans. Jobs at the scanner group level are broken down into tasks when there is available capacity. Tasks from those jobs can then be divided among the scanners in the group.
Job Queues

Tenable.io queues scan jobs before separating them into tasks for scan distribution.

Scanner Group Job Queues

Tenable.io queues jobs for a scanner group in the order it receives the jobs. When the scanner group has available job capacity, Tenable.io breaks the earliest job in the queue into tasks and assigns them to each of the scanners in the group, one scanner after another in succession (a “round robin” method). Tenable.io dispatches the tasks to the scanners assigned to the job.

Scanner Job Queues

Tenable.io also queues jobs for a scanner in the order it receives the jobs, regardless of the origin of a scan job.

For example, the job queue for a scanner may include scan jobs that were assigned directly to the scanner as well as jobs distributed to the scanner by the groups the scanner belongs to.
Dispatching Tasks

When a scanner has available capacity for tasks, it polls for and is assigned additional tasks from the jobs that have filled the scanner’s job capacity. Tasks are assigned from each job in succession, in a round robin method, similar to the way jobs are assigned to scanners in a group.

The way the tasks are dispatched to scanners varies depending on the scenario.

Example Scenario: One Scanner with One Job

In this example, assume there is one scanner with a single job queued. This scanner is not a part of a scanner group and as such processes scan jobs one at a time in the order the jobs are queued. This scanner has a task capacity of six. When the job is broken down into tasks, six of those tasks are assigned to the scanner to be executed simultaneously. Tasks continue to fill the scanner’s task capacity until the scan job is completed.

Example Scenario: One Scanner with Multiple Jobs

In this example, assume there is one scanner with multiple jobs queued. The scanner belongs to two scanner groups, SG1 and SG2. Three scan jobs are created. The first scan was configured to use the scanner directly. The other two scans were configured to use SG1 and SG2, respectively.

Because the first scan job was configured to use that particular scanner, it is added to the scanner’s job queue. In the case of SG1 and SG2, the scanner happens to be next in the order of scanners to receive jobs in both groups. The jobs from those groups are also added to the scanner’s job queue.

This scanner has a job capacity of three, so the scanner is able to be assigned tasks from all three jobs.

This scanner has a task capacity of five. Tasks are assigned to the scanner one at a time from each job in succession. In this case, tasks would be assigned in the following order: Job 1, Job 2, Job 3, Job 1, Job 2, filling the task capacity. Using this “round robin” method, the scanner begins working on two tasks from the first job, two tasks from the second job, and one task from the third job. When one of the tasks is completed, the next task from the third job is then dispatched.

Example Scenario: Multiple Scanners with Multiple Jobs

In this example, assume there are two scanners, Scanner 1 and Scanner 2. Both scanners are assigned to a scanner group, SG1. Both Scanner 1 and Scanner 2 have a job capacity of three.
Two scan jobs are created. Job 1 is assigned directly to Scanner 1. Job 2 is assigned to SG1. Both Jobs are broken down into Tasks. Job1 will only be worked by Scanner 1. Job 2 can be worked by both Scanner 1 and Scanner 2.

Both Scanner 1 and Scanner 2 have a task capacity of six. Scanner 1 is assigned tasks one at a time from each job in succession, three from Job 1 and three from Job 2. Scanner 2 is assigned six tasks from Job 2.

Tasks for Job 2 are dispatched to Scanner 1 and Scanner 2 from SG1 as task capacity becomes available for the scanners. This process continues until both jobs are completed.
WAS Scanning Overview

**Required Additional License:** Tenable.io Web Application Scanning

**Note:** The topics in this section describe web application scans in the new interface only. If you activate the new interface, you can view a historical snapshot of scan configurations in the classic interface, but you can modify those configurations in the new interface only. For information about scans in the classic interface, see [Scans (Classic Interface)](#).

Configure web application scans to collect data about your web applications for analysis. This overview walks you through the main steps you need to create, configure, launch, and manage web application scans.

Depending on your organization, one person may perform all of the steps, or several people may share the steps.

Create and launch a web application scan

1. **Create** a web application scan.
2. Select a scan template that fits your needs.
   - Use a [Tenable-provided scan template](#).
   - Create and use a [user-defined scan template](#).
3. Configure the scan:
   - Configure the [scan settings](#) available for your scan template.
   - (Optional) To run a credentialed scan, [configure credentials](#).
4. **Launch** the scan.
   - Monitor the [scan status](#).
   - View details about the scan's efficiency in the [Notes tab](#).

View and manage scans
1. **View** your scan results.

2. **View** details about the plugin results in attachments to scan results.

3. Remove legacy scans and scan results from your dashboard.

   - **Delete the results** from a single scan job.
   - **Move a Scan to the Trash Folder** a scan and the associated results to the **Trash** folder.
   - **Delete a scan**, along with all the scan results for that scan.
CS Scanning Overview

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable.io Container Security

Configure Tenable.io Container Security scans to collect data about your containers for analysis. Depending on your organization, one person may perform all of the steps, or several people may share the steps.

To configure Tenable.io Container Security scans:

1. Import and scan your container images.
   - If you want to upload a specific image to Tenable.io Container Security for scanning, download the image from your external registry and push the image to Tenable.io Container Security.
   - If you want to import all the images from a registry to Tenable.io Container Security for scanning, configure a connector to import images from a registry.

   **Note:** If you use a connector to import and scan your images, Tenable.io Container Security may take up to several hours to display your images on the dashboard. If your images do not appear on the dashboard within 24 hours of when you begin the import, contact Tenable Support.

   - If you want to scan an image directly from your organization’s local registry, or from your machine, download and run the Tenable.io CS Scanner.

The amount of time Tenable.io Container Security takes to scan the images in your registry and display the results depends on the size and number of images you scan.

**Note:** The data Tenable.io Container Security retains when you import an image depends on the import method you use.

- **Docker command** or **connector** – Tenable.io Container Security retains the image itself, as well as all metadata associated with the image (e.g., image layers, software packages on the image., etc.).
• **Tenable.io CS Scanner** – Tenable.io Container Security retains only the metadata associated with the image. When you [delete the image](#), Tenable.io Container Security removes the entire image and all image metadata.

2. Navigate the Tenable.io Container Security [dashboard](#) to view and manage your scan data.

**Note:** Tenable.io Container Security imports and rescans your images at regular intervals, beginning when you first import and scan the images.
Log in to CS via the Docker CLI

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable.io Container Security

You can use a Docker command to log in to Tenable.io Container Security Scanner to push images via the Docker command line interface (CLI).

To navigate the interface and use other features, log in via the Tenable.io interface. For more information, see [Log in to Tenable.io](#).

Before you begin:

- Obtain credentials for your Tenable.io user account.

  **Note:** If you are an administrator logging in to your Tenable.io instance for the first time, Tenable provides your first-time credentials during setup. After you log in for the first time, you can set your new password. If you are logging in to Tenable.io after initial setup, your username is the email address you used to register for your Tenable.io account.

- Review the [System Requirements](#) in the General Requirements User Guide and confirm that your computer and browser meet the requirements.

To log in to Tenable.io Container Security via a Docker command:

1. Generate your API access and secret keys.
2. In the Docker CLI, run the following command:

   ```bash
docker login registry.cloud.tenable.com
   ```

   The CLI prompts you to provide a username.

3. Type your API access key.

4. Press **Enter**.

   The CLI prompts you to provide a password.
5. Type your API secret key.

6. Press Enter.

The Docker CLI logs you in to the Tenable.io Container Security registry.
Push a Container Image to CS

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Required Additional License: Tenable.io Container Security

Required Tenable.io Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

Use Docker commands to download the image from the external registry where it resides and import it to Tenable.io Container Security.

The amount of time Tenable.io Container Security takes to scan the images in your registry and display the results depends on the size and number of images you scan.

Before you begin:

- Log in to Tenable.io Container Security via the Docker command.

To push container image to Tenable.io Container Security:

1. Use the `docker pull` command to download the image from an external registry.

   ```
   docker pull alpine:latest
   ```

2. Use the `docker tag` command to add the `registry.cloud.tenable.com` tag.

   ```
   docker tag alpine:latest registry.cloud.tenable.com/alpine:latest
   ```

   **Note:** The `registry.cloud.tenable.com` tag prompts Docker to push the image to Tenable.io Container Security. If you do not add the `registry.cloud.tenable.com` tag, Docker automatically pushes the image to the Docker central repository.

3. Use the `docker push` command to push the tagged image to Tenable.io Container Security.

   ```
   docker push registry.cloud.tenable.com/alpine:latest
   ```
Docker pushes the image to Tenable.io Container Security. Tenable.io Container Security scans the images for vulnerabilities.

**Note:** When you import container images to scan, Tenable.io Container Security may abort the scan if the scan has been running for 60 minutes. If this happen, *Scan Failed* appears on the Images page in the Vulnerabilities and Malware columns for the aborted images.

If Tenable.io Container Security aborts your scan, try simplifying your images before you import them, as described in the Docker Documentation. Alternatively, you can use the Tenable.io CS Scanner to scan your images without importing them to Tenable.io Container Security.

If Tenable.io Container Security still aborts your scan, contact Tenable Support.

What to do next:

- View the results of your scan, as described in View Scan Results for Container Images.
Push from Bamboo to CS

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Required Additional License: Tenable.io Container Security

Before You Begin

These instructions describe how to push a Docker image from Bamboo to Tenable.io Container Security.

These steps assume you are already comfortable using Bamboo and are already pushing Docker images to a public or private registry. If you are already using Bamboo, but have not built Docker container images, familiarize yourself with the Bamboo documentation Configuring the Docker task in Bamboo.

Steps

1. Create a new Docker task for the relevant job.
2. In the Task box, type a description for the task.
3. Depending on whether you want the task to run, select or clear the Disable this task check box.
4. Select Push a Docker image to a Docker registry command and complete the settings.

   Bamboo builds are sent to Tenable.io Container Security for storage, distribution, vulnerability scanning, and malicious code scanning.
Push from CircleCI to CS

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Required Additional License: Tenable.io Container Security

Before You Begin

These instructions describe how to push a Docker image from CircleCI to Tenable.io Container Security.

These steps assume you are already comfortable using CircleCI and are already pushing Docker images to a public or private registry. If you are already using CircleCI, but have not built Docker container images, familiarize yourself with the CircleCI documentation Continuous Integration and Delivery with Docker.

Click here for information about the circle.yml file.

If you are using CircleCI to build Docker container images, you should have a circle.yml file in your project source control repository that looks similar to the following example:

```yaml
machine:
services:
  - docker

dependencies:
  override:
  - docker info
  - docker build -t circleci/elasticsearch

test:
  override:
  - docker run -d -p 9200:9200 circleci/elasticsearch; sleep 10
  - curl --retry 10 --retry-delay 5 -v http://localhost:9200

deployment:
hub:
```
The following lines in `circle.yml` instruct CircleCI to leverage Docker for the build process:

```
branch: master
commands:
- docker push circleci/elasticsearch
```

The following lines in `circle.yml` instruct CircleCI to build the `elasticsearch` image in the `circleci/` repository:

```
machine:
services:
- docker

dependencies:
override:
- docker info
- docker build -t circleci/elasticsearch
```

The following are the most important lines for adding Tenable.io Container Security integration to CircleCI environments. These lines instruct CircleCI to use Docker to log in to the registry (in this case to Docker Hub, since no private registry is specified) and push `circleci/elasticsearch` to the registry:

```
deployment:
hub:
branch: master
commands:
- docker login -u $DOCKER_USER -p $DOCKER_PASS
- docker push circleci/elasticsearch
```

**Steps**

1. To add environment variables for the project in the CircleCI console, open the project, click **Project Settings**, then click **Environment Variables**.
2. Define the following variables:
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TENABLE_IO_CONTAINER_SECURITY_EMAIL</td>
<td>The email that you use to log in to Tenable.io Container Security.</td>
</tr>
<tr>
<td>TENABLE_IO_CONTAINER_SECURITY_USER</td>
<td>The user name that you use to log in to Tenable.io Container Security. You can find this on the <strong>Settings</strong> page in Tenable.io Container Security.</td>
</tr>
<tr>
<td>TENABLE_IO_CONTAINER_SECURITY_ENDPOINT</td>
<td>For hosted cloud users of Tenable.io Container Security, this value is registry.cloud.tenable.com.</td>
</tr>
</tbody>
</table>

3. To add support for Tenable.io Container Security, update the `circle.yml` file as follows:

```yaml
machine:
environment:
  VERSION: 2.1.1
  TAG: ${VERSION}
services:
  - docker

dependencies:
  override:
  - docker info
  - docker version
  - docker build -t $TENABLE_IO_CONTAINER_SECURITY_ENDPOINT/circleci/elasticsearch .

test:
  override:
  - docker run -d -p 9200:9200 $TENABLE_IO_CONTAINER_SECURITY_ENDPOINT/circleci/elasticsearch; sleep 10
  - curl --retry 10 --retry-delay 5 -v registry.cloud.tenable.com

deployment:
hub:
```
branch: master
commands:
- docker login -u $TENABLE_IO_ACCESS_KEY -p $TENABLE_IO_SECRET_KEY
- docker tag $TENABLE_IO_CONTAINER_SECURITY_ENDPOINT/circleci/elasticsearch $TENABLE_IO_CONTAINER_SECURITY_ENDPOINT/circleci/elasticsearch:${TAG}
- docker push $TENABLE_IO_CONTAINER_SECURITY_ENDPOINT/circleci/elasticsearch:${TAG}
- docker logout

CircleCI builds are sent to Tenable.io Container Security for storage, distribution, vulnerability scanning, and malicious code scanning.
Push from Codeship to CS

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Required Additional License: Tenable.io Container Security

Before You Begin

These instructions describe how to push a Docker image from Codeship to Tenable.io Container Security.

These steps assume you are already comfortable using Codeship and are already pushing Docker images to a public or private registry. If you are already using Codeship, but have not built Docker container images, familiarize yourself with the Codeship documentation Pushing to a remote registry.

Steps

1. Edit the codeship-services.yml file to use the repository name and image name specified in Tenable.io Container Security.

```
app:
  build:
    image: repository_name/image_name
    dockerfile_path: Dockerfile
```

**Note:** If this is the first time you are pushing an image into the repository, there is not a preconfigured image name. The image name is added automatically after the push from Codeship.

2. Edit the service section of the the codeship-steps.yml file to look similar to the following example:

```
service:
  app type: push
  image_name: repository_name/image_name
  registry: registry.cloud.tenable.com
```
encrypted_dockercfg_path: dockercfg.encrypted

Codeship builds are sent to Tenable.io Container Security for storage, distribution, vulnerability scanning, and malicious code scanning.
Push from Distelli to CS

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Required Additional License: Tenable.io Container Security

Before You Begin

These instructions describe how to push a Docker image from Distelli to Tenable.io Container Security using the Distelli WebUI Manifest.

These steps assume you are already comfortable using Distelli and are already pushing Docker images to a public or private registry. If you are already using Distelli, but have not built Docker container images, familiarize yourself with the Distelli documentation on the Distelli Manifest. You can use the Distelli manifest file by either using the Distelli WebUI Manifest, or by editing the distelli-manifest.yml file directly.

Steps

1. Log in to Distelli and navigate to an application.

2. Click the Manifest tab.

   The Build section displays content similar to the following example:

   ```
   docker build --quiet=false -t $DOCKER_REPO:$DISTELLI_BUILDNUM .
   docker login -u $DOCKER_USERNAME -p $DOCKER_PW
   docker push $DOCKER_REPO:$DISTELLI_BUILDNUM
   ```

3. To add support for Tenable.io Container Security, modify the Build section to look like the following example:

   ```bash
   bash docker build --quiet=false -t $TENABLE_IO_CONTAINER_SECURITY_REPO:$DISTELLI_BUILDNUM .
   docker login -u $TENABLE_IO_ACCESS_KEY -p $TENABLE_IO_SECRET_KEY
   registry.cloud.tenable.com docker push $TENABLE_IO_CONTAINER_SECURITY_REPO:$DISTELLI_BUILDNUM
   ```
This modification adds the Tenable.io Container Security URI to docker login.

Distelli builds are sent to Tenable.io Container Security for storage, distribution, vulnerability scanning, and malicious code scanning.
Push from Drone.io to CS

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable.io Container Security

Before You Begin

These instructions describe how to push a Docker image from Drone.io to Tenable.io Container Security.

These steps assume you are already comfortable using Drone.io and are already pushing Docker images to a public or private registry. For more information about Drone.io, see the [Drone.io Documentation](#).

If you use Drone.io to build Docker container images, you should already have a build script (usually a `build.sh` file) that looks like the following:

```
$ docker build -t docker-registry/image-name .
$ docker push docker-registry/image-name
```

Steps

1. Open the `build.sh` file.

2. Append a docker login directive before the docker push directive in the script, as in the following example:

```
$ docker build -t docker-registry/image-name .
$ docker login -u $TENABLE_IO_ACCESS_KEY -p $TENABLE_IO_SECRET_KEY registry.cloud.tenable.com
$ docker push docker-registry/image-name
```

Drone.io builds for this project are sent to Tenable.io Container Security for storage, distribution, vulnerability scanning, and malicious code scanning.
Push from Jenkins to CS

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable.io Container Security

**Before You Begin**

These instructions describe how to push a Docker image from Jenkins to Tenable.io Container Security.

These steps assume you are already comfortable using Jenkins and are already pushing Docker images to a public or private registry. If you are already using Jenkins, but have not built Docker container images, familiarize yourself with the documentation for the Jenkins [CloudBees Docker Build and Publish plugin](https://plugins.jenkins.io/cloudbees-docker).

Click here for instructions on how to install the CloudBees Docker Build and Publish plugin.

1. Log in to Jenkins.
2. Click Manage Jenkins, then click Manage Plugins.
3. Click Installed.
   
   A list of installed plugins appears.
4. Click Available.
5. In the Filter box, type CloudBees Docker Build and Publish plugin.
6. Select the check box that corresponds to the plugin.
7. Install the plugin.

The CloudBees Docker Build and Publish plugin is installed and ready for use by Jenkins jobs.

**Steps**
1. On the Jenkins dashboard, select the job you want to modify.

2. Click **Configure**.

3. In the **Build** section, click **Add build step**.

4. In the drop down box, select **Docker Build and Publish**.

5. Type the details for the following configuration parameters:

   - **Repository Name:** The repository name and image name. For example, if you build a rabbitmq container image, you can name the repository rabbitmq and the image rabbitmq. In this example, in the **Repository Name** box, type `rabbitmq/rabbitmq`.

   - **Tag:** The tag name. The simplest tag name to use is `latest`.

   - **Docker Host URI:** The Jenkins path to the Docker Host. If the Docker Host is running on localhost, then in the **Docker Host URI** box, type `tcp://127.0.0.1:4243`.

   - **Docker registry URL:** The Tenable.io Container Security API endpoint, which in this case is `registry.cloud.tenable.com`.

   - **Registry credentials:** The registry credentials that you select from the box.

   **Adding registry credentials**

   1. Click **Add**.

   2. Click **Username with password**.

   3. In the **Username** box, type your Tenable.io Container Security user name.

   4. In the **Password** box, type your Tenable.io Container Security password.

   5. Click **Add**.

      The credentials are added.

6. Click **Save**.

   Jenkins builds are sent to Tenable.io Container Security for storage, distribution, vulnerability scanning, and malicious code scanning.
Push from Shippable to CS

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Required Additional License: Tenable.io Container Security

Before You Begin

These instructions describe how to push a Docker image from Shippable to Tenable.io Container Security.

These steps assume you are already comfortable using Shippable and are already pushing Docker images to a public or private registry. If you are already using Shippable, but have not built Docker container images, familiarize yourself with the Shippable documentation Building a Docker image.

Steps

1. Log in to Shippable.
2. In the upper right corner of the screen, click the Account Settings button.
3. Click Integrations, and then click Add Integration.
4. In the Master Integration section, click Private Docker Registry.
5. In the Name box, type Tenable.io Container Security.
6. In the URL box, type registry.cloud.tenable.com.
7. In the Username box, type your Tenable.io Container Security user name.
8. In the Password box, type your Tenable.io Container Security password.
9. In the Email box, type the email address associated with your Tenable.io Container Security account.
10. Click Save.

Your Tenable.io Container Security account is now available for hosting container images built by Shippable.
11. Access your project page, and click **Settings**.

12. Click **Hub**, and select the Tenable.io Container Security integration that you just created.

13. In the **Push Build** field, click **Yes**.

14. In the **Push image to** box, type the name of your repository and image in Tenable.io Container Security (e.g., testrepo/nodejs).

15. In the **Push Image Tag** box, select from the following options: **default**, **commitsha**, or **latest**.

16. Click **Save**.

   Shippable builds are sent to Tenable.io Container Security for storage, distribution, vulnerability scanning, and malicious code scanning.
Push from Solano Labs to CS

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Required Additional License: Tenable.io Container Security

Before You Begin

These instructions describe how to push a Docker image from Solano Labs to Tenable.io Container Security.

These steps assume you are already comfortable using Solano Labs and are already pushing Docker images to a public or private registry. If you are already using Solano Labs, but have not built Docker container images, familiarize yourself with the Solano Labs documentation.

Note: Solano Labs support for building Docker container images is in private beta. For customers interested in participating, Solano Labs recommends contacting Solano Labs support.

Steps

1. Open the solano.yml file, which should look similar to the following example:

```yaml
# Use docker-enabled workers (currently private beta - contact support@solanolabs.com)
system:
docker: true
python:
python_version: 2.7
hooks:
pre_setup: |
  set -ex
  sudo apt-get update -qq
  sudo docker pull jenkins
  sudo docker build -t myrepo/jenkins-dsl-ready:my .
tests:
  - python -m doctest build/resolve_jenkins_plugins_dependencies.py
```
2. Add a post_build phase with your Tenable.io Container Security user name.

```bash
# Use docker-enabled workers (currently private beta - contact support@solanolabs.com)
system:
docker: true
python:
python_version: 2.7
hooks:
pre_setup: |
  set -ex
  sudo apt-get update -qq
  sudo docker pull jenkins
  sudo docker build -t myrepo/jenkins-dsl-ready
post_build: |
  docker login -u $TENABLE_IO_ACCESS_KEY -p $TENABLE_IO_SECRET_KEY
  registry.cloud.tenable.com
  docker push myrepo/jenkins-dsl-ready
tests:
  - python -m doctest build/resolve_jenkins_plugins_dependencies.py
```

Solano Labs builds are sent to Tenable.io Container Security for storage, distribution, vulnerability scanning, and malicious code scanning.
**Push from Travis CI to CS**

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable.io Container Security

**Before You Begin**

These instructions describe how to push a Docker image from Travis CI to Tenable.io Container Security.

These steps assume you are already comfortable using Travis CI and are already pushing Docker images to a public or private registry. If you are already using Travis CI, but have not built Docker container images, familiarize yourself with the Travis CI documentation [Using Docker in Builds](#).

Click here for information about the `travis.yml` file.

If you are using Travis CI to build Docker container images, you should have a `travis.yml` file in your project source control repository that looks similar to:

```yaml
sudo: required
language: ruby
services:
  - docker
before_install:
  - docker build -t carlad/sinatra .
  - docker run -d -p 127.0.0.1:80:4567 carlad/sinatra /bin/sh -c "cd /root/sinatra; bundle exec foreman start;"
  - docker ps -a
  - docker run carlad/sinatra /bin/sh -c "cd /root/sinatra; bundle exec rake test"
script:
  - bundle exec rake test

The following lines in `travis.yml` instruct Travis CI to leverage Docker for the build process:

```yaml
sudo: required
services:
  - docker

The following lines in `travis.yml` instruct Travis CI to build the sinatra image in the carlad/ repository:

```yaml
sudo: required
services:
  - docker
Steps

1. Open the `travis.yml` file.


   ```
   $ travis encrypt TENABLE_IO_CONTAINER_SECURITY_EMAIL=email@organization.com
   $ travis encrypt TENABLE_IO_CONTAINER_SECURITY_USER=username
   $ travis encrypt TENABLE_IO_CONTAINER_SECURITY_PASSWORD=password
   ```

3. Add your environment variables.

   ```
   env:
   global:
   - secure: "UkF2CHX01UZ...VI/LE=" # TENABLE_IO_CONTAINER_SECURITY_EMAIL
   - secure: "Z3fdBNPt5hR...VI/LE=" # TENABLE_IO_CONTAINER_SECURITY_USER
   - secure: "F4XbD6WybHC...VI/LE=" # TENABLE_IO_CONTAINER_SECURITY_PASSWORD
   - COMMIT=${TRAVIS_COMMIT::8}
   ```

4. Add your connection information.

   ```
   after_success:
   - docker login -u $TENABLE_IO_CONTAINER_SECURITY_EMAIL -p $TENABLE_IO_CONTAINER_SECURITY_PASSWORD registry.cloud.tenable.com
   - export REPO=web-login-site/web-login-site
   - export TAG='if [ "$TRAVIS_BRANCH" == "master" ]; then echo "latest"; else echo "$TRAVIS_BRANCH"; fi'
   - docker build -f Dockerfile -t $REPO:$COMMIT .
   - docker tag $REPO:$COMMIT registry.cloud.tenable.com/$REPO:$TAG
   - docker tag $REPO:$COMMIT registry.cloud.tenable.com/$REPO:travis-$TRAVIS_BUILD_NUMBER
   - docker push registry.cloud.tenable.com/$REPO:travis-$TRAVIS_BUILD_NUMBER
   - docker push registry.cloud.tenable.com/$REPO:$TAG
   ```

Travis CI builds are sent to Tenable.io Container Security for storage, distribution, vulnerability scanning, and malicious code scanning.
Push from Wercker to CS

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Required Additional License: Tenable.io Container Security

Before You Begin

These instructions describe how to push a Docker image from Wercker to Tenable.io Container Security.

These steps assume you are already comfortable using Wercker and are already pushing Docker images to a public or private registry. If you are already using Wercker, but have not built Docker container images, familiarize yourself with the Wercker documentation Containers.

Steps

1. In your project source control repository, open the wercker.yml file.

2. Add support for Tenable.io Container Security by changing the deploy directive as follows:

```yaml
deploy:
  steps:
    - internal/docker-push:
      username: $USERNAME
      password: $PASSWORD
      tag: my-amazing-tag
      repository: turing/bar
      registry: registry.cloud.tenable.com
```

Wercker builds for this project are sent to Tenable.io Container Security for storage, distribution, vulnerability scanning, and malicious code scanning.
The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

You can run the Tenable.io Container Security Scanner with Kubernetes to securely scan container images without sending the images outside your organization's network. For more information, see Tenable.io CS Scanner.

- [Tenable.io CS Scanner System Requirements for Kubernetes](#)
- [Prepare Kubernetes Objects to Configure and Run the Tenable.io CS Scanner](#)
- [Configure and Run the Tenable.io CS Scanner in Kubernetes](#)
Tenable.io CS Scanner System Requirements for Kubernetes

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

The machine where you want to run the Tenable.io Container Security Scanner with Kubernetes must meet the following requirements:

Software and Hardware Requirements

<table>
<thead>
<tr>
<th>Software Requirements</th>
<th>RAM</th>
<th>Temporary Storage</th>
<th>CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Able to run Linux containers</td>
<td>2 GiB</td>
<td>15 GB</td>
<td>1.5 GHz</td>
</tr>
</tbody>
</table>

Internet

The machine where you want to run the Tenable.io CS Scanner must have access when you download and run the scanner.

SSL Certificate Requirements

If the registry that hosts your images requires the HTTPS protocol, you must have an SSL certificate signed by a trusted Certificate Authority (CA) installed on the registry. Refer to your registry's documentation for installing an SSL certificate.

Note: Mozilla's CA Certificate Store is the Tenable.io Container Security Scanner's trusted certificate authority.

Note: If you want the Tenable.io CS Scanner to scan the registry without verifying that a trusted CA signed the certificate, you must include the ALLOW_INSECURE_SSL_REGISTRY variable when you run the scanner. For more information, see Environment Variables.
Prepare Kubernetes Objects to Configure and Run the Tenable.io CS Scanner

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable.io Container Security

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

You must prepare your Kubernetes namespace and secret objects before you can configure and run the Tenable.io CS Scanner in Kubernetes. The Tenable.io CS Scanner refers to these objects when it scans an image in Kubernetes.

Secrets contain sensitive information associated with the TENABLE_ACCESS_KEY, TENABLE_SECRET_KEY, REGISTRY_USERNAME, and REGISTRY_PASSWORD environment variables described in [Environment Variables](#). To run the Tenable.io CS Scanner in Kubernetes, you must configure these secrets and deploy them to the registry where the image you want to scan is stored.

For more information about how to create objects in Kubernetes, see the Kubernetes documentation at [kubernetes.io](http://kubernetes.io).

Before you begin:

- Download the Tenable.io CS Scanner, as described in [Download the CS Scanner](#).

To prepare Google Kubernetes Engine (GKE) to configure and run the Tenable.io CS Scanner:

1. Log in to the CLI on the machine where you want to configure and run the Tenable.io CS Scanner.

2. In a text editor, create a namespace file (`tiocsscanner-namespace.yaml`) for your CS Scanner. A `tiocsscanner-namespace.yaml` file is provided below.
3. Save and close the file.

4. Deploy the `tiocssscanner-namespace.yaml` file to GKE using the command below:

```bash
kubectl apply -f tiocssscanner-namespace.yaml
```

Your namespace is configured and deployed.

**Note:** The above command works only if the file is saved to the current working directory. If the file is saved somewhere other than the working directory, include the full path directory in the command. For example:

```bash
kubectl apply -f /home/jsmith/images/tiocssscanner-namespace.yaml
```

5. Configure secrets for your Tenable.io access and secret keys. For example:

```bash
kubectl create secret generic tio
  --from-literal=username=<Your Tenable.io access key>
  --from-literal=password=<Your Tenable.io secret key>
  --namespace=tiocssscanner
```

Your Tenable.io access key and secret key secrets are configured.

6. Configure secrets for your Google Container Registry (GCR) registry username and password (obtained from step 3 and 4 in [Prepare your GCP GCR](#)) for the image you want the scanner to pull. For example:

```bash
kubectl create secret generic gcr-registry
  --from-literal=username=<Your gcr registry username>
  --from-literal=password=<Your gcr registry password>
  --namespace=tiocssscanner
```
Your private registry username and password secrets are configured.

7. Deploy your secrets to the registry where the image you want to scan is stored. For example:

Configure secrets for the registry where the Tenable.io Container Security scanner image is stored. For example:

```bash
kubectl create secret docker-registry jfrog-tio \
--docker-server=https://tenableio-docker-consec-local.jfrog.io \
--docker-username=<tenable jfrog username obtained from the Tenable.io Container Security console> \
--docker-password=<tenable jfrog password obtained from the Tenable.io Container Security console> \
--docker-email=<Your email address> \
--namespace=tio-csscanner
```

Your secrets are deployed to the registry.

What to do next:

- Configure and run the Tenable.io CS Scanner in Kubernetes, as described in [Configure and Run the CS Scanner in Kubernetes](#).
Configure and Run the Tenable.io CS Scanner in Kubernetes

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable.io Container Security

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

To scan images with the Tenable.io CS Scanner in Kubernetes, create a Kubernetes deployment file and deploy the file via the CLI on the machine where you want to run the scan.

Before you begin:

- Confirm your machine meets the system requirements, as described in [Tenable.io CS Scanner System Requirements](#).
- Download the Tenable.io CS Scanner, as described in [Download the Tenable.io CS Scanner](#).
- Prepare Kubernetes to configure and run the Tenable.io CS Scanner, as described in the [Prepare Kubernetes Objects to Configure and Run the Tenable.io CS Scanner](#).

To deploy Tenable.io CS Scanner to Google Kubernetes Engine (GKE):

1. In a text editor, open a new file.
2. Save the file as `tiocsscanner-deployment.yaml`.
3. Copy and paste the text below into the `tiocsscanner-deployment.yaml` file, typing your specific variables where applicable. For information about the following variables, see [Environment Variables](#).

   **Note:** The sample `tiocsscanner-deployment.yaml` file provided below generally works for Google Kubernetes Engine (GKE) with Google Cloud Registry (GCR). You may need to change the value of `apiVersion`, depending on which version of Kubernetes you are using.
tiocsscanner-deployment.yaml

```yaml
apiVersion: v1
kind: Service
metadata:
  name: tiocsscanner
  namespace: tiocsscanner
  labels:
    app: tiocsscanner
spec:
  selector:
    app: tiocsscanner
  type: ClusterIP
  ports:
    - name: http
      protocol: TCP
      port: 5000
---
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  labels:
    app: tiocsscanner
  name: tiocsscanner
  namespace: tiocsscanner
spec:
  minReadySeconds: 10
  replicas: 1
  selector:
    matchLabels:
      app: tiocsscanner
  strategy:
    rollingUpdate:
      maxSurge: 1
      maxUnavailable: 1
      type: RollingUpdate
  template:
    metadata:
      labels:
        app: tiocsscanner
    spec:
      imagePullSecrets:
        - name: jfrog-tio
      containers:
        - image: "tenableio-docker-consec-local.jfrog.io/cs-scanner:latest"
          name: tiocsscanner
          resources:
            limits:
              cpu: "3"
            requests:
              cpu: "1.5"
              memory: "2Gi"
          args:
            - import-registry
          env:
```

---

---

---

---

---
- name: TENABLE_ACCESS_KEY
  valueFrom:
    secretKeyRef:
      name: tio
      key: username
- name: TENABLE_SECRET_KEY
  valueFrom:
    secretKeyRef:
      name: tio
      key: password
- name: REGISTRY_USERNAME
  valueFrom:
    secretKeyRef:
      name: gcr-registry
      key: username
- name: REGISTRY_PASSWORD
  valueFrom:
    secretKeyRef:
      name: gcr-registry
      key: password
- name: IMPORT_REPO_NAME
  value: "<variable>"
- name: REGISTRY_URI
  value: "https://[gcr-domain]/[project]"
- name: IMPORT_INTERVAL_MINUTES
  value: "<variable>"

Note: If your project name in GCP is myapigw and the registry is in the gcr.io domain, the value of REGISTRY_URI will be "https://gcr.io/myapigw".

4. Save and close the file.

5. In the CLI on the machine where you want to run the scan, type the following to deploy the file:

   ```bash
   kubectl apply -f tiocssscanner-deployment.yaml
   ```

   Note: The above command works only if the file is saved to the current working directory. If the file is saved somewhere other than the working directory, include the full path directory in the command. For example:

   ```bash
   /home/jsmith/images/tiocssscanner-namespace.yaml
   ```

6. Press Enter.

   The Tenable.io CS Scanner runs on Kubernetes.

7. Run the following command to confirm the scan ran successfully:
kubectl get pods --namespace=tioasscanner

The scan status log appears.

**Note:** If you receive error messages in the scan data, follow the error prompts to correct the issue.

What to do next:

- View the results of your scan, as described in [View Scan Results for Container Images](#).
The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

The Tenable.io Container Security Scanner (Tenable.io CS Scanner) allows you to securely scan container images without sending the images outside your organization's network. The Tenable.io CS Scanner takes an initial inventory, or snapshot, of the images you want to scan and sends the inventory to Tenable.io for analysis. You can then view scan data for the images alongside data for images imported normally to Tenable.io. With the Tenable.io CS Scanner, you can scan:

- A specific image exported from a registry and stored locally on the machine where you install the scanner.
- All images hosted in a specific registry (e.g., a Docker registry).

You can configure and run the Tenable.io CS Scanner on any machine that meets the system requirements.

First, download the Tenable.io CS Scanner to your machine. Then, configure and run the Tenable.io CS Scanner. After your scan completes, you can view the scan results in the Tenable.io Container Security dashboard.
The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

The machine where you want to run the Tenable.io Container Security Scanner must meet the following requirements.

### Software and Hardware Requirements

<table>
<thead>
<tr>
<th>Deployment Type</th>
<th>Software Requirements</th>
<th>RAM</th>
<th>Temporary Storage</th>
<th>CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>Able to run Linux containers</td>
<td>2 GB</td>
<td>15 GB</td>
<td>64-bit multi-core, x86 compatible</td>
</tr>
</tbody>
</table>

### Internet

The machine where you want to run the Tenable.io CS Scanner must have access to the Internet when you download and run the scanner.

### SSL Certificate Requirements

If the registry that hosts your images requires the HTTPS protocol, you must have an SSL certificate signed by a trusted Certificate Authority (CA) installed on the registry. Refer to your registry's documentation for installing an SSL certificate.

**Note:** Mozilla's CA Certificate Store is the Tenable.io Container Security Scanner's trusted certificate authority.

**Note:** If you want the Tenable.io CS Scanner to scan the registry without verifying that a trusted CA signed the certificate, you must include the ALLOW_INSECURE_SSL_REGISTRY variable when you run the scanner. For more information, see Environment Variables.

### Supported Container Image Formats

The Tenable.io CS Scanner supports the following image formats:
• Docker images

• Open Containers Initiative (OCI) images
Download the Tenable.io CS Scanner

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable.io Container Security

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

Download the Tenable.io CS Scanner Docker image to the machine where you want to configure and run the Tenable.io CS Scanner.

Before you begin:

- Confirm your machine meets the system requirements, as described in [CS Scanner System Requirements](#).

To download the CS Scanner:

1. In the **Connectors** section of the **Container Security** dashboard, click **Create**.
   
   The **Select a Connector** plane appears.

2. Under **CONTAINER SECURITY**, click **CS Scanner**.
   
   The **CS Scanner** plane appears with login credentials.

3. Copy or take a screenshot of the credentials to use later in the download process.

4. In the command line interface (CLI) on the machine where you want to download the Tenable.io CS Scanner, type:

   ```
   docker login tenableio-docker-consec-local.jfrog.io
   ```

5. Press **Enter**.
   
   The CLI prompts you to provide a username and password.

6. Update the fields using the credentials provided on the **CS Scanner** plane.
7. **Press Enter.**

   You are logged in to the Tenable.io CS Scanner.

8. Type the following to pull the latest version of the Tenable.io CS Scanner image:

   ```
docker pull tenableio-docker-consec-local.jfrog.io/cs-scanner:latest
```

9. Press **Enter**.

What to do next:

- Configure and run the Tenable.io CS Scanner, as described in [Configure and Run the Tenable.io CS Scanner](#).
You must use the CLI on your computer to configure your environment variables and run the Tenable.io CS Scanner.

You can configure and run the Tenable.io CS Scanner as many times as necessary, using any combination of registries and registry sources.

### Environment Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Type</th>
<th>Required</th>
<th>Supported Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>TENABLE_ACCESS_KEY</td>
<td>Your Tenable.io API access key.</td>
<td>String</td>
<td>Yes</td>
<td>Image Inspect or Registry Import</td>
</tr>
<tr>
<td>TENABLE_SECRET_KEY</td>
<td>Your Tenable.io API secret key.</td>
<td>String</td>
<td>Yes</td>
<td>Image Inspect or Registry Import</td>
</tr>
<tr>
<td>IMPORT_REPO_NAME</td>
<td>The name of the Tenable.io CS Scanner repository where you want to import the image. This name cannot contain spaces. The repository name must meet the following requirements: • Contains 64 characters or fewer.</td>
<td>String</td>
<td>Yes</td>
<td>Image Inspect or Registry Import</td>
</tr>
<tr>
<td><strong>REGISTRY_URI</strong></td>
<td>The URI of the registry from which you want to import the image.</td>
<td>String</td>
<td>No</td>
<td>Registry Import</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------</td>
<td>--------</td>
<td>----</td>
<td>-----------------</td>
</tr>
<tr>
<td><strong>REGISTRY_USERNAME</strong></td>
<td>Your username for authenticating to the registry you want to scan. Set this variable if you want to authenticate to the registry. The username you provide must be for an account with privileges to import and scan registries in the Tenable.io CS Scanner. Your username variable depends on the registry you want to scan:</td>
<td>String</td>
<td>No</td>
<td>Registry Import</td>
</tr>
<tr>
<td></td>
<td>• Amazon Web Services (AWS) Elastic Container Registry (ECR) — Type your AWS access key ID as your username. For information about how to obtain your access key ID, see the AWS Documentation.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Azure registry — Type your service principal ID for the registry. For more information about how to create a service principal, see Azure</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Documentation.

- Google Cloud Platform (GCP) Google Container Registry (GCR) – Type your GCR account client email as it appears in the client_email field in the service account private key JSON file. For information about how to create and download your service account private key, see the Google Container Registry Documentation.

- All other registries – Type the username you use to authenticate to the registry.

| REGISTRY_PASSWORD | Your password for authenticating to the registry from which you want to import the image. Set this variable if you want to authenticate to the registry. The password you provide must be for an account with privileges to import and scan registries in the Tenable.io CS Scanner. Your password depends on the registry you want to scan. • Amazon Web Services (AWS) Elastic Container Registry (ECR) – Type your AWS access secret key as your password. For information about how to obtain your access | String | No | Registry Import |
- **secret key**, see the *AWS Documentation*.

- **Azure registry** – Type your service principal password for the registry. For more information about how to create a service principal, see *Azure Documentation*.

- **Google Cloud Platform (GCP) Google Container Registry (GCR)** – Type your GCR service account private key as it appears in the `private_key` field in the service account private key JSON file. For information about how to create and download your service account private key, see the *Google Container Registry Documentation*.

- **All other registries** – Type the password you use to authenticate to the registry.

### | TENABLE_PROXY | The URL for the HTTP proxy the Tenable.io CS Scanner uses to connect to Tenable.io. Set this variable if the machine where you deployed the Tenable.io CS Scanner requires a proxy server to connect to Tenable.io. | String | No | Image Inspect or Registry Import
---|---|---|---|---|---

**Note:** If the machine where you deployed the Tenable.io CS Scanner requires proxy...
connections to your registry and to Tenable.io, you can apply both the REGISTRY_PROXY variable and the TENABLE_PROXY variable to your configuration. Run the Tenable.io CS Scanner in Registry Import mode if you apply both variables.

Your TENABLE_PROXY variable depends on whether your proxy requires username and password authentication.

- **Authentication required** – Type your proxy URL in the following format:

  `<username>:<password>@<host>:<port>`

- **Authentication not required** – Type your proxy URL in the following format:

  `<host>:<port>`

**Note:** You can specify the host using the hostname (for example, example.com) or IP address (for example 192.0.2.202).

| REGISTRY_PROXY | The URL for the HTTP proxy the Tenable.io CS Scanner uses to connect to your registry. Set this variable if the machine where you deployed the Tenable.io CS Scanner requires a proxy server to connect to the registry you want to scan. | String | No | Registry Import |
**Note:** If the machine where you deployed the Tenable.io CS Scanner requires proxy connections to your registry and to Tenable.io, you can apply both the REGISTRY_PROXY variable and the TENABLE_PROXY variable to your configuration.

Your REGISTRY_PROXY variable depends on whether your proxy requires username and password authentication.

- Authentication required – Type your proxy URL in the following format:
  ```
  <username>:<password>@<host>:<port>
  ```

- Authentication not required – Type your proxy URL in the following format:
  ```
  <host>:<port>
  ```

**Note:** You can specify the host using the hostname (for example, example.com) or IP address (for example 192.0.2.202).

<table>
<thead>
<tr>
<th>IMAGE_NAME_WHITELIST</th>
<th>Description</th>
<th>Type</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Image name or tag assigned to images that you want the Tenable.io CS Scanner to include in your registry scan. Include this variable if you want to run the Tenable.io CS Scanner in Registry Import mode and you want the scanner</td>
<td>String</td>
<td>No</td>
</tr>
</tbody>
</table>

Registry Import
to include only images with a certain name or tag in the scan.

If you do not set this variable, Tenable.io CS Scanner scans all the images in your registry.

**Note:** You cannot include an IMAGE_NAME_WHITELIST variable and an IMAGE_NAME_BLACKLIST variable in the same scan configuration.

Your whitelist variable depends on whether you want to include images based on name, tag, or both.

- **Name** – Type the name assigned to images that you want included in the scan.

  For example, if you type `-e IMAGE_NAME_WHITELIST=alpine`, the Tenable.io CS Scanner scans only images named alpine.

- **Tag** – Type the tag assigned to images that you want included in `*:<tag>` format.

  For example, if you type `-e IMAGE_NAME_WHITELIST-T=*:latest`, the Tenable.io CS Scanner scans only images with the latest tag.

- **Both** – Type the image name and tag set assigned to images that you want included in `<image>:<tag>`.
For example, if you type `-e IMAGE_NAME_WHITELIST-T=alpine:latest`, only images named alpine that also have the latest tag are included in the scan.

**Tip:** You can use an asterisk (*) wild card character when specifying image name and tag values.

**Tip:** You can specify multiple whitelist variables by separating each with a comma (for example, `-e IMAGE_NAME_WHITELIST-T=alpine1,alpine2,alpine3,*:latest`).

<table>
<thead>
<tr>
<th>IMAGE_NAME_WHITELIST</th>
<th>Image name or tag assigned to images that you want the Tenable.io CS Scanner to exclude from your registry scan.</th>
</tr>
</thead>
<tbody>
<tr>
<td>image_name_</td>
<td>No</td>
</tr>
<tr>
<td>Registry Import</td>
<td>No</td>
</tr>
</tbody>
</table>

Include this variable if you want to run the Tenable.io CS Scanner in Registry Import mode and you want the scanner to exclude certain images from the scan. If you do not set this variable, Tenable.io CS Scanner scans all the images in your registry.

If you do not set this variable, Tenable.io CS Scanner scans all the images in your registry.

**Note:** You cannot include an IMAGE_NAME_BLACKLIST variable and an IMAGE_NAME_WHITELIST variable in the same scan configuration.
Your blacklist variable depends on whether you want to exclude images based on name, tag, or both.

- **Name** – Type the name assigned to images that you want excluded from the scan.

  For example, if you type `-e IMAGE_NAME_BLACKLIST=alpine`, the Tenable.io CS Scanner excludes only images named alpine.

- **Tag** – Type the tag assigned to images that you want excluded from the scan in `*:<tag>` format.

  For example, if you type `-e IMAGE_NAME_BLACKLIST-T=*:latest`, the Tenable.io CS Scanner excludes only images with the latest tag.

- **Both** – Type the image name and tag set assigned to images you want excluded in `<image>:<name>` format.

  For example, if you type `-e IMAGE_NAME_BLACKLIST-T=alpine:latest`, only images named alpine that also have the latest tag are excluded from the scan.
| **Tip:** | You can use an asterisk (*) wild card character when specifying image name and tag values. |
| **Tip:** | You can specify multiple blacklist variable sets by separating each set with a comma (for example, `-e IMAGE_NAME_BLACKLIST=alpine1,alpine2,alpine3,*:latest`). |
| **CHECK_POLICY** | If true, the Tenable.io CS Scanner sends a request to Tenable.io to verify whether the results of the scan include a violation of one or more compliance policies. The message that Tenable.io CS Scanner provides in the output log depends on the results of the policy check. |
| | • Policy violation detected – Tenable.io CS Scanner provides the following message: *This image does not pass your compliance policy.* |
| | • No policy violation detected – Tenable.io CS Scanner provides the following message: *Image has passed your policy compliance.* |
| | • Policy check timed out – Tenable.io CS Scanner provides the following message: *Fatal error: Timed out trying to retrieve report.* |

| **Boolean** | No | Image Inspect |
If the policy check fails for any reason other than a policy violation or a policy check timeout, the Tenable.io CS Scanner generates a message specific to the error that caused the failure.

**Tip:** If you write custom code to automate image scanning via the Tenable.io CS Scanner, you can refer to the following exit codes to determine whether the image passed the policy check:

- 0 – The image passed the policy check.
- 1 – The policy check failed, due to timeout or some other error.
- 2 – The image failed the policy check and is in violation or one or more compliance policies.

For information about Tenable.io Container Security policies, see Manage CS Policies.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Type</th>
<th>Default</th>
<th>Example</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHECK_POLICY_TIMEOUT</td>
<td>The amount of time, in seconds, that the Tenable.io CS Scanner waits for Tenable.io to finish scanning the image and complete the vulnerability detection analysis. By default, the Tenable.io CS Scanner times out unanswered request for a policy after 600 seconds.</td>
<td>Integer</td>
<td>No</td>
<td>Image Inspect</td>
<td></td>
</tr>
<tr>
<td>IMPORT_</td>
<td>The frequency, in minutes, you want the</td>
<td>Integer</td>
<td>No</td>
<td>Registry</td>
<td></td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Type</td>
<td>Default</td>
<td>Mode</td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>---------</td>
<td>---------------</td>
<td></td>
</tr>
<tr>
<td>INTERVAL_MINUTES</td>
<td>Tenable.io CS Scanner to import and scan images from the selected registry. Set this variable if you want the scanner to run repeatedly at set intervals. If you do not set this variable, the Tenable.io CS Scanner imports and scans images from the selected registry only the first time you scan your registry.</td>
<td></td>
<td></td>
<td>Import</td>
<td></td>
</tr>
<tr>
<td>DEBUG_MODE</td>
<td>If true, the Tenable.io CS Scanner adds additional information to the scan's log to assist with debugging.</td>
<td>Boolean</td>
<td>No</td>
<td>Image Inspect or Registry Import</td>
<td></td>
</tr>
<tr>
<td>ALLOW_INSECURE_SSL_REGISTRY</td>
<td>If true, the Tenable.io CS Scanner accepts the registry's SSL certificate without verifying that a trusted Certificate Authority (CA) issued the certificate.</td>
<td>Boolean</td>
<td>No</td>
<td>Registry Import</td>
<td></td>
</tr>
</tbody>
</table>
| HTTP_CONNECTION_TIMEOUT_SECONDS | The amount of time, in seconds, that the Tenable.io CS Scanner waits for a response after sending a connection request to the registry. If the registry does not accept the connection request within this time span, Tenable.io CS Scanner cancels (times out) the request.

By default, the Tenable.io CS Scanner times out unanswered connection requests after 10 seconds. | Integer | No | Image
Inspect or
Registry Import |
| HTTP_IDLE_TIMEOUT_SECONDS | The amount of time, in seconds, that the Tenable.io CS Scanner waits for a response after sending a request for image data to the registry. If the registry does not respond within this time limit, the Tenable.io CS Scanner cancels (times out) the request.

By default, the Tenable.io CS Scanner times out unanswered requests after 60 seconds. | Integer | No | Image
Inspect or
Registry Import |
| HTTP_REQUEST_TIMEOUT_SECONDS | The amount of time, in seconds, that the Tenable.io CS Scanner allows a request to remain active (i.e., the amount of time the Tenable.io CS Scanner waits for the registry to accept a connection request and respond to a request for image data). If a request is still active after this time limit has passed, the Tenable.io CS Scanner cancels (times out) the request. | Integer | No | Image
Inspect or
Registry Import |
| By default, the Tenable.io CS Scanner times out active requests after 60 seconds. |   |   |
Configure and Run the Tenable.io CS Scanner

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

When you run the Tenable.io Container Security Scanner, you can configure it to scan a single image or all images hosted in a repository.

- To scan a single image, configure and run the Tenable.io CS Scanner in Image Inspect mode.
- To scan all images in a registry, configure and run the Tenable.io CS Scanner in Registry Import mode.
Scan an Image via the Tenable.io CS Scanner

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable.io Container Security

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

Run the Tenable.io CS Scanner in Image Inspect mode to scan a single image.

Before you begin:

- Download the image you want to scan to your local machine.
- Confirm your local machine meets the system requirements, as described in CS Scanner System Requirements.
- Download the Tenable.io CS Scanner, as described in Download the CS Scanner.
- Prepare your environment variable value, as described in Environment Variables.

To run the Tenable.io CS Scanner in Image Inspect mode:

1. In the CLI of the machine where you want to run the scanner, type the customized configuration and command for your deployment type using the parameters defined below.

   **Note:** Some of the following variables are not required to run the scanner. For information about these variables and their definitions, see Environment Variables.

   ```bash
docker save <your image name as it appears in the repository> | docker run \
-e TENABLE_ACCESS_KEY=<variable> \
-e TENABLE_SECRET_KEY=<variable> \
-e IMPORT_REPO_NAME=<variable>
```
2. Press **Enter**.

   The Tenable.io CS Scanner scans the image.

What to do next:

- View the results of your scan, as described in [View Scan Results for Container Images](#).
Scan a Registry via the Tenable.io CS Scanner

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable.io Container Security

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

Run the Tenable.io CS Scanner in Registry Import mode to scan all images in a registry.

Before you begin:

- Confirm your machine meets the system requirements described in [Tenable.io CS Scanner System Requirements](#).
- Download the Tenable.io CS Scanner, as described in [Download the CS Scanner](#).
- Obtain registry credentials for an account with privileges to import and scan a registry.
- Prepare your environment variable values, as described in [Environment Variables](#).
- (Optional) To scan images hosted in an Amazon Web Services (AWS) Elastic Container Registry (ECR), an Azure registry, or a Google Container Registry (GCR), prepare your registry as described in [Prepare your Registry](#).

To run the Tenable.io CS Scanner in Registry Import mode:

1. In the CLI of the machine where you want to run the scanner, type the customized configuration and command for your deployment type using the parameters defined below.

   ```
   docker run \
   -e TENABLE_ACCESS_KEY=<variable> \
   ```

   **Note:** Some of the following variables are not required to run the scanner. For information about these variables and their definitions, see [Environment Variables](#).
2. Press **Enter**.

   The Tenable.io CS Scanner scans all images in the registry.

**What to do next:**

- View the results of your scan, as described in [View Scan Results for Container Images](#).
Prepare your Registry

**Required Additional License:** Tenable.io Container Security

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

You must prepare the following registries before you scan the registries via the Tenable.io CS Scanner.

- Amazon Web Service (AWS) Elastic Container Registry (ECR)
- Azure Registry
- Google Cloud Platform (GCP) Google Container Registry (GCR)

You do not need to prepare other registry types before scanning.

**Amazon Web Service (AWS) Elastic Container Registry (ECR)**

For information about how to make specific configurations to your AWS ECR, see the *AWS Documentation*.

To prepare your AWS ECR:

1. Configure your AWS ECR.
2. Obtain your AWS access keys.

**Note:** Your AWS access keys consist of two parts: an access key ID and an access secret key. The access key ID is your registry username variable, and the secret access key is your registry password variable. For more information, see *Tenable.io CS Scanner Environment Variables*.

What to do next:

- Scan your repository, as described in *Scan a Registry via the Tenable.io CS Scanner*.

**Azure Registry**

For information about how to make specific configurations to your Azure registry, see the *Azure Documentation*.
To prepare your Azure registry:

1. Configure your Azure registry.
2. Create a service principal for your Azure registry and assign the AcrPull role to the service principal.

What to do next:

- Scan your repository, as described in Scan a Registry via the Tenable.io CS Scanner.

Google Cloud Platform (GCP) Google Container Registry (GCR)

For information about how to make specific configurations to your GCP GCR, see the Google Container Registry Documentation.

To prepare your GCP GCR:

1. Create a service account in GCR with the Project Viewer role.
2. Authenticate to your registry by creating and downloading a service account key as a JSON file. A sample is provided below.

```json
{
  "type": "service_account",
  "project_id": "my-gcp-lab",
  "private_key_id": "d21bbxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
  "private_key": "-----BEGIN PRIVATE KEY-----
MIIEvAAA...END PRIVATE KEY-----"
,  "client_email": "cs-scanner@my-gcp-lab.iam.gserviceaccount.com",
  "client_id": "111111111111111111",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://oauth2.googleapis.com/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
  "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/cs-scanner%40dh-lab.iam.gserviceaccount.com"
}
```

3. Mount the service account JSON file to the path /serviceAccount.json using the docker -v flag:

```bash
docker run -e TENABLE_ACCESS_KEY=<redacted> \
```

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
What to do next:

- Scan your repository, as described in [Scan a Registry via the Tenable.io CS Scanner](#).
## Glossary of CS Terms

Tenable.io Container Security product documentation uses the following terms:

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CD System</td>
<td>A Continuous Deployment system. Typically used to monitor for successful builds that have passed tests, and to take those successful builds and push them to production environments, thus automating the deployment of the successful builds.</td>
</tr>
<tr>
<td>CI System</td>
<td>A Continuous Integration system. Typically used to monitor source control commits, such as merged pull requests in GitHub, to automatically trigger a build (to test) as the change in source control is detected.</td>
</tr>
<tr>
<td>CI/CD System</td>
<td>A Continuous Integration and Continuous Deployment system. Typically used to monitor source control commits, such as merged pull requests in GitHub, to automatically trigger a build (to test) as the change in source control is detected, and upon successful completion of the build and test phase, to take those successful builds and push them to production environments, thus automating the deployment of the successful build.</td>
</tr>
<tr>
<td>Container</td>
<td>A running instance of a container image. A container image that has been started or otherwise executed.</td>
</tr>
<tr>
<td>Container Image</td>
<td>An application hosted inside of a container image file (for example, ubuntu:14.04).</td>
</tr>
<tr>
<td>Container Image Tag</td>
<td>A specific release or version of an application hosted inside of a container (for example, 14.04).</td>
</tr>
<tr>
<td>Container Registry</td>
<td>A storage location for Container Images. Provides developers and continuous integration systems the ability to store containers that are pushed.</td>
</tr>
<tr>
<td>Continuous Deployment</td>
<td>A development practice where operations (or DevOps) automatically push successfully tested builds to production environments, making them immediately available.</td>
</tr>
<tr>
<td>Continuous</td>
<td>A development practice where developers integrate code into a shared</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Integration</td>
<td>source control repository, regularly, as changes are made.</td>
</tr>
<tr>
<td>Image</td>
<td>An application hosted inside of a container image file (for example, ubuntu:14.04).</td>
</tr>
<tr>
<td>Image Tag</td>
<td>A specific release or version of an application hosted inside of a container (for example, 14.04).</td>
</tr>
<tr>
<td>Organization Admin</td>
<td>The role assigned to the first user registering for Tenable.io Container Security, at the time the Organization is created. If you have registered without an invitation, you were automatically assigned the role of Organization Admin and a new Organization was created for your account.</td>
</tr>
<tr>
<td>Registry</td>
<td>A storage location for Container Images. Provides developers and continuous integration systems the ability to store containers that are pushed.</td>
</tr>
<tr>
<td>Repository</td>
<td>A storage location or namespace, within the registry, for an image (for example, /org/tenable_io_container_security/approved/).</td>
</tr>
<tr>
<td>Tag</td>
<td>A specific release or version of an application hosted inside of a container (for example, 14.04).</td>
</tr>
<tr>
<td>User</td>
<td>The role assigned to invited users registering for Tenable.io Container Security, for pre-existing Organizations. If you have registered via an invitation, you were automatically assigned the role of User and you were added to the same Organization of the user who invited you.</td>
</tr>
</tbody>
</table>
PCI ASV Scanning Overview

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Tip:** This topic describes PCI ASV scans in the new interface. For information about the classic interface, see [PCI ASV Scans (Classic Interface)](#). For information about navigating the new interface, see [Navigate Tenable.io](#) (New Interface).

Credit card industry standards dictate that companies whose networks process payment card transactions must scan those networks for Payment Card Industry Data Security Standards (PCI DSS) compliance at regular intervals. Additionally, these companies must submit their scan results to a third-party Approved Scanning Vendor (ASV) for review.

Tenable.io PCI ASV scan templates allow you take comprehensive scans of your networks so you can identify and address vulnerabilities and ensure your organization complies with PCI DSS.

Tenable is also a licensed ASV reviewer, providing the external scanning and validation that PCI Security Standards require.

The Tenable.io PCI ASV process strictly follows PCI Compliance Guidelines, ensuring that vulnerabilities do not exist for more than 90 days on any networks that involve payment card transactions.

To prepare for a PCI ASV review:

1. Work with your organization to determine what assets in your cardholder data environment (CDE) are in scope for PCI/ASV scanning and review.

2. Create the following scans:
   - [Create a scan](#) with the **PCI Quarterly External Scan** template.
   - [Create a Web Application scan](#) using the **PCI** template. This scan should be run on payment pages, web application pages, or any pages that can be seen as entry into the CDE or that may contain Card Holder Data (CHD).

**Note:** PCI scan data is intentionally excluded from dashboards, reports, and workbenches. This is due to the scan's paranoid nature, which may lead to false positives that would otherwise not be detected.
Note: Because PCI ASV scans using the PCI Quarterly External Scan and PCI template have their own set of rules, any recast rules do not apply to the scan results.

Note: PCI DSS requires organizations to complete quarterly internal network scans, so you may also need to create a scan using the PCI Internal Network Scan template. However, you do not need to submit the internal network scan results for ASV review and validation.

3. **Launch** the scan.

Note: Since a clean scan substantially increases your chances to pass the ASV certification review, Tenable recommends that you launch the PCI ASV scan as many times as is needed to get the cleanest scan possible.

4. **Submit the scan** to the PCI ASV dashboard.

5. **Create an attestation** request draft. As you create the draft, you may need to do one or both of the following:

   - If your scan results include assets that are irrelevant to the attestation, **mark each irrelevant asset out of scope**.
   
   - If the scan results include any failures, create a **dispute** for each failure.

   Note: If you leave any failures undisputed when you submit your attestation for review, the ASV reviewer must fail the attestation.

6. After you have addressed all the failures, **submit the scan attestation for ASV review**.
Submit a Scan to the PCI ASV Dashboard

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

After you create and launch your PCI ASV, you must import the scan to the PCI ASV scans table to start the review and attestation process.

Before you begin:

- [Create a scan](#) using the appropriate PCI ASV scan template. For information about PCI ASV scan templates, see [PCI ASV Scanning Overview](#).
- [Launch](#) the scan.

To submit a scan to the PCI ASV dashboard:

1. In the upper-left corner, click the ** button.
   
   The left navigation plane appears.

2. In the left navigation plane, in the **Vulnerability Management** section, click **Scans**.
   
   The **Scans** page appears.

3. In the **Folders** section, click a folder to load the scans you want to view.
   
   The scans table updates to display the scans in the folder you selected.

4. In the scans table, click the scan you want to import to the PCI ASV dashboard.
   
   The **Scans Details** page appears.

5. Click **Submit for PCI**.
   
   Tenable.io imports the scan to the PCI ASV dashboard.

What to do next:

- [Create an attestation](#) for the scan.
Create an Attestation

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

After you submit a PCI ASV scan to the PCI ASV dashboard, you must create an attestation request draft.

**Note:** When you create an attestation request draft for a scan, you do not also submit the scan for ASV attestation. You must dispute all remaining failures and address all out of scope assets before you submit the attestation for ASV approval.

**Caution:** You cannot create an attestation for scans that are more than 90 days old.

To create an attestation request:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. Click **PCI ASV**.
   
   The **PCI ASV** page appears, displaying a scans table.

3. In the scans table, in the **New Scan Results** tab, select the check box next to the scan or scans for which you want to create an attestation.

4. In the lower-right corner of the page, click **Start New Attestation**.
   
   The **Attestation Detail** page appears.

5. In the **Name** box, type the name of the attestation as you want it to appear on the attestation request.

   **Note:** Tenable recommends that you type a name you can easily identify. After you submit the attestation request, you cannot change the name on the attestation.

6. (Optional) To assign the attestation to a different user, in the **Owner** drop-down box, select the user to whom you want to assign the attestation.
7. Click **Save**.

Tenable.io saves the attestation draft in the **In Remediation** tab of the PCI ASV table.

**Note:** You can return to a saved, unsubmitted attestation and configure the options until you submit the attestation for review.

What to do next:

- If the scan includes any assets that are irrelevant to the PCI ASV review, **mark each irrelevant asset out of scope**.
- If the new attestation displays any failures in the **Undisputed Failures** tab, **create a dispute** for each failure.
Mark an Asset as Out of Scope

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

Before you begin:

- [Create](#) and [launch](#) your scan.
- [Create an attestation request](#) for your scan.

To mark an asset as out of scope:

1. In the upper-left corner, click the ** button.
   
   The left navigation plane appears.

2. Click **PCI ASV**.
   
   The **PCI ASV** page appears, displaying a scans table.

3. Click the **In Remediation** tab.
   
   A table of your attestation requests appears.

4. Click the attestation that has an asset you want to mark out of scope.
   
   The **Attestation Details** page appears.

5. Click the **Assets** tab.
   
   A table of assets associated with the attestation appears.

6. Select the check box next to the asset or assets you want to mark out of scope.
   
   In the lower-right corner, the **Mark as Out of Scope** button appears.

7. Click the **Mark as Out of Scope** button.
   
   Tenable.io removes the asset or assets from PCI ASV review scope.

What to do next:
• If your attestation request includes any undisputed failures, create a dispute for each failure.

• If your attestation request has no undisputed failures, submit the attestation request for ASV review.
Disputes

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

When you create and launch a PCI ASV scan, the scan results may include findings you want to dispute before you submit the associated attestation for review. To address these findings, you can create a dispute to submit to the ASV reviewer.

After you create a dispute, you can edit, clone, or delete the dispute as needed.

- Create a Dispute
- Clone a Dispute to an Attestation
- Edit a Dispute
- Delete a Dispute
Create a Dispute

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Required User Role: Administrator

When you run a PCI scan and the scan detects failures, you must dispute the failures before you can submit the associated attestation for ASV review.

Before you begin:

- Create an Attestation for the scan.
- (Optional) To remove certain assets from the PCI ASV review, mark each asset as out of scope.

To create a dispute:

1. In the upper-left corner, click the button.
   The left navigation plane appears.
2. Click PCI ASV.
   The PCI ASV page appears, displaying a scans table.
3. Click the In Remediation tab.
   A table of your attestation requests appears.
4. Click the attestation that has a failure you want to dispute.
   The Attestation Details page appears.
5. Click the Undisputed Failures tab.
   A table of the undisputed failures for the attestation appears.
6. Do one of the following:
To create one dispute:

a. Roll over the row for the failure you want to dispute.

   The button appears next to the plugin name.

b. Click the button.

   The New Dispute page appears.

To create multiple disputes:

a. Select the check box next to each failure you want to dispute.

b. In the lower-right corner, click New Dispute.

   The New Dispute page appears.

   **Note:** You can create a single dispute for multiple failures only if all the failures have the same plugin ID.

7. In the **Name** box, type a name for the dispute.

   **Note:** By default, a concatenation of the IP address and plugin ID associated with the failure appears in the Name box.

8. (Optional) To assign the dispute to a different user, in the **Owner** drop-down box, select the user you to whom you want to assign the dispute.

9. In the **Reason** drop-down box, select the reason for the dispute. For details on each reason, see Dispute Reasons.

10. In the **Explanation** text box, type an explanation for the dispute.

    **Note:** You can click the plugin ID to get more information about the failure and use the information in your explanation.

11. (Optional) To add an external file as evidence to support your dispute, do the following:
• In the **Evidence** section, click **Add File**.

  An explorer window appears.

• Select the file you want to add to your dispute.

**Note:** PCI ASV supports the following file types for evidence attachments:

- .bmp
- .csv
- .db
- .gif
- .jpeg
- .jpg
- .json
- .nessus
- .pdf
- .png
- .txt

When you upload a file as evidence, PCI ASV automatically saves the uploaded file to the dispute before you click **Save** or **Cancel**.

12. (Optional) To add more files to the dispute, repeat the previous step.

**Note:** You can add as many files as you want to a dispute as long as the total file size does not exceed 10 GB.

13. Click **Save**.

  Tenable.io saves your dispute to the attestation.

  A **Dispute Successfully Submitted** notification momentarily appears.

  Your dispute appears in the **Disputes** tab.

**What to do next:**

• (Optional) To change details of the dispute, [edit the dispute](#).

• (Optional) To remove the dispute from your attestation, [delete the dispute](#).
Edit a Dispute

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

**Note:** You cannot edit a dispute after you submit the attestation for ASV review.

To edit a dispute:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. Click **PCI ASV**.
   
   The **PCI ASV** page appears, displaying a scans table.

3. Click the **In Remediation** tab.
   
   A table of your attestation requests appears.

4. Click the attestation that has a dispute you want to edit.
   
   The **Attestation Details** page appears.

5. Click the **Disputes** tab.
   
   A table of your disputes appears.

6. Click the dispute you want to edit.
   
   The **Edit Dispute** page appears.

7. Configure the options you want to change. For information about the options, see [Create a Dispute](#).

8. Click **Save**.
   
   Tenable.io saves your edits to the dispute.
Clone a Dispute to an Attestation

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

You can clone a dispute and add it to an attestation that you previously submitted for ASV review.

**Note:** When you clone a dispute into an attestation, any other disputes attached to the same attestation are deleted.

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. Click **PCI ASV**.
   
   The **PCI ASV** page appears, displaying a scans table.

3. Click the **In Remediation** tab.
   
   A table of your attestation requests appears.

4. Click the attestation that has a dispute you want to clone into a previously submitted attestation.
   
   The **Attestation Detail** page appears.

5. In the upper-right corner, click **Clone Disputes**.
   
   The **Clone Disputes** page appears.

   **Note:** Only attestations that you previously submitted for ASV validation appear in the table.

6. Click the row that contains the attestation you want to clone the dispute from.
   
   The **Disputes to Clone** plane appears and displays the disputes that will be cloned from the attestation.
7. Click **Clone**.

A *Disputes successfully cloned* message appears and Tenable.io clones the dispute into the attestation.
Delete a Dispute

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

**Note:** You cannot delete a dispute after you submit the attestation associated to the dispute for ASV review.

To delete a dispute:

1. In the upper-left corner, click the button.
   
The left navigation plane appears.

2. Click **PCI ASV**.
   
The **PCI ASV** page appears, displaying a scans table.

3. Click the **In Remediation** tab.
   
   A table of your attestation requests appears.

4. Click the attestation that includes a dispute you want to delete.
   
The **Attestation Details** page appears.

5. Click the **Disputes** tab.
   
   A table of your disputes appears.

6. Do one of the following:

   • **To delete one dispute:**
     
     a. Roll over the row for the dispute you want to delete.
        
        The button appears next to the last modified date.

     b. Click the button.
A confirmation window appears, prompting you to confirm you want to delete the dispute.

- To delete multiple disputes:
  a. Select the check box next to each dispute you want to delete.
  b. In the lower-right corner, click **Delete**.

A confirmation window appears, prompting you to confirm you want to delete the dispute.

7. Click **Delete**.

Tenable.io deletes the dispute.
**Dispute Reasons**

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Before you submit your PCI ASV attestation for review, you may want to dispute detected failures in the PCI ASV scan. When you dispute a failure, you must select an appropriate reason and provide an explanation.

When filing a PCI ASV dispute, you can select one of the following reasons:

1. **False Positive**
2. **Compensating Controls**
3. **Exception**

**False Positive**

It’s possible that after patching or fixing all reported vulnerabilities, as defined by the PCI DSS compliance standards, you have a failure in your scan report that doesn’t apply to the host. False positives can occur due to rapid changes in vendor-specific updates or backported patches that aren’t easily detected by banner checks.

For example, a scan may report that a critical patch is missing from a host; however, the patch is actually installed. If a false positive occurs, you can provide proof of the false positive by uploading a screen capture, configuration file, or other supporting data as evidence. Evidence must be accompanied by a description of when, where, and how the evidence was obtained.

**Compensating Controls**

Compensating controls may be considered for most PCI DSS requirements if, due to legitimate technical or documented business constraints, you cannot meet a requirement as stated. You can, however, sufficiently mitigate the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:
• They must meet the intent and rigor of the original PCI DSS requirement.

• They must provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against.

Tip: You can check the Guidance Column for the intent of each PCI DSS requirement in the Payment Card Industry (PCI) Data Security Standard specification document.

• They must go "above and beyond" other PCI DSS requirements. Simply being compliant with other PCI DSS requirements does not constitute a compensating control.

For example, if you are unable to render cardholder data unreadable per Requirement 3.4 (for example, by encryption), a compensating control could consist of a device or combination of devices, applications, and controls that address all of the following:

• internal network segmentation

• IP address or MAC address filtering

• one-time passwords

Note: The Payment Card Industry (PCI) Data Security Standard specification document provides a compensating controls worksheet in Appendix C.

Exception

A dispute can still be filed for a failure that is not a false positive or if compensating controls are not in place. An exception must be supported by evidence that the failure does not pose a risk to the Cardholder Data Environment (CDE). Common exceptions include disputed CVSS base scores or PCI ASV scans that cannot be completed due to scan interference.
Submit an Attestation for ASV Review

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Required User Role: Administrator

Before you begin:

- Create an attestation for the scan you want to submit for ASV review.
- If your attestation includes assets that are not in scope for the PCI ASV review, mark each irrelevant asset as out of scope.
- If your attestation includes undisputed failures, create a dispute for each failure.

To submit an attestation for ASV review:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. Click PCI ASV.
   
   The PCI ASV page appears, displaying a scans table.

3. In the In Remediation tab, click the attestation you want to submit for ASV review.
   
   The Attestation Details page appears.

4. (Optional) To update the name of the attestation, in the General Information tab, in the Name box, type a new name.

5. (Optional) To update the owner of the attestation, in the General Information tab, in the Owner drop-down box, select the owner you want to assign to the attestation.
6. Do one of the following:

   - Fix any undisputed failures before submitting the attestation:
     a. On the Undisputed Failures tab, create a dispute for each failure.
     b. Click Submit to ASV Review.

   - Submit the attestation with known failures.

   **Note**: You may want to submit an attestation with undisputed failures if you need guidance on handling these failures, or if you need to obtain an initial attestation with a list of identified failures.

   **Caution**: If you submit an attestation that has undisputed failures to ASV for review, the ASV reviewer must fail the attestation.

     a. Click Submit to ASV Review.

        The Submit for ASV Review panel appears.

     b. In the Select the reason for submitting this scan drop-down, select the reason you want to submit the scan with known failures.

     c. In the Comments box, provide any additional information on why you want to submit the scan with known failures.

     d. Click Submit Scan.

        The Attestation Detail page appears.

7. On the Attestation Detail page, configure the attestation information:

   a. In the Contact Name box, type a contact for the attestation.

   b. In the Email box, type an email for the attestation contact.

   c. In the Phone box, type a phone number for the attestation contact.

   d. In the Job Title box, type a job title for the attestation contact.

   e. In the Company box, type the company where the attestation contact works.

   f. In the Web URL box, type the URL for the company’s website.
g. In the **Address Line 1** box, type the address of the company.

h. (Optional) In the **Address Line 2** box, type any additional address information for the company, such as a suite number or floor number.

i. In the **City** box, type the city where the company is located.

j. In the **State / Province / Region** box, type the state, province, or region where the company is located.

k. In the **Zip / Postal Code** box, type the zip code for the company’s address.

l. (Optional) To add the country where the company is located, in the **Country** box, type the country.

8. In the **Attestation Agreement** section, carefully read the terms of the attestation agreement.

9. Click **Attest**.

An **Attestation Successfully Submitted for ASV Review** success notification appears, and Tenable.io adds the attestation to the **In Review** tab.

After the ASV review completes the review, the attestation appears under the **In Review** tab. If the attestation passed, a ✓ icon appears in the row. If the attestation failed, a ☐ icon appears in the row.

**Note:** Once your attestation moves to the **In Review** or **Attestation** tab, the attestation is read-only. You cannot make additional changes to the attestation unless an ASV reviewer initiates an information request.

**Tip:** After you create your first attestation request, the **New Attestation** screen automatically populates the above fields with your previously entered information in each subsequent attestation request.

What to do next:

- If the ASV reviewer requests additional information about your disputed failures, respond to the requests. For more information, see **Respond to an ASV Review Information Request**.
Respond to an ASV Review Information Request

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

If you have any disputed failures in your attestation request when you submit the attestation for ASV review, the ASV reviewer may ask for additional information.

You can respond to the reviewer directly in the dispute.

Before you begin:

- Submit your attestation for ASV review.

To respond to an information request:

1. In the upper-left corner, click the ☰ button.
   
   The left navigation plane appears.

2. Click **PCI ASV**.
   
   The **PCI ASV** page appears, displaying a scans table.

3. Click the **In ASV Review** tab.
   
   A table of your attestation requests appears.

4. Locate the attestation that has an ▲ icon next to the **Owner**.

5. Click the attestation.
   
   The **Attestation Details** page appears.

6. Click the **Disputes** tab.
   
   A table of your disputes appears.

7. Click the dispute that has an ▲ icon next to the reason.
   
   The dispute details page appears.
8. In the **Explanation** section, view the question or comment the ASV reviewer submitted.

9. Do one of the following:
   - To submit a text-based response to the ASV reviewer, in the **Explanation** section, in the text box, type your response.
   - To add a file as evidence to support your dispute:
     a. In the **Evidence** section, click **Add File**.
        An explorer window appears.
     b. Select the file you want to add to your dispute.
        
        **Note:** PCI ASV does not restrict the file types you add to a dispute. Additionally, when you upload a file as evidence, PCI ASV automatically saves the file to the dispute before you click Save or Cancel.
     c. (Optional) To add more files to the dispute, repeat the previous step.
        
        **Note:** You can add as many files as you want to a dispute as long as the total file size does not exceed 10 GB.

10. Click **Save**.

    A **Dispute Successfully Submitted** notification momentarily appears.

    Tenable.io submits your response to the ASV reviewer.

    **Note:** You cannot edit or delete a response after you submit it to the ASV reviewer.

11. Repeat steps 7-10 for each dispute in the **Disputes** tab that has an ⚫ icon next to the reason.
PCI ASV Scans (Classic Interface)

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Tip: This topic describes PCI ASV scans in the classic interface. For information about the new interface, see PCI ASV Scanning Overview.

Credit card industry standards dictate that companies whose networks process payment card transactions must scan those networks for Payment Card Industry Data Security Standards (PCI DSS) compliance at regular intervals. Additionally, these companies must submit their scan results to a third-party Approved Scanning Vendor (ASV) for review.

Tenable.io PCI ASV scan templates allow you to take comprehensive scans of your networks so you can identify and address vulnerabilities and ensure your organization complies with PCI DSS.

Tenable is also a licensed ASV reviewer, providing the external scanning and validation that PCI Security Standards require.

The Tenable.io PCI ASV process strictly follows PCI Compliance Guidelines, ensuring that vulnerabilities do not exist for more than 90 days on any networks that involve payment card transactions.

Video: PCI ASV High Level Workflow in Tenable.io

To prepare for a PCI ASV review:

1. Work with your organization to determine what assets in your cardholder data environment (CDE) are in scope for PCI/ASV scanning and review.

2. Create a scan with the PCI Quarterly External Scan template.

Note: Because the PCI Quarterly External scan is more paranoid than standard scans and may lead to false positives, your PCI scan data is intentionally excluded from your overall Tenable.io scan data.

Note: Because PCI ASV scans using the PCI Quarterly External Scan template have their own set of rules, any recast rules do not apply to the scan results.
3. If your organization’s assets include web applications that are in scope for the PCI/ASV review, **create a scan** using the **PCI WAS Scan** template.

**Note**: The **PCI WAS Scan** template is available only in the classic Tenable.io interface.

4. **Launch** the scan.

**Note**: Since a clean scan substantially increases your chances to pass the ASV certification review, Tenable recommends that you launch the PCI ASV scan as many times as is needed to get the cleanest scan possible.

5. **Submit the scan** to the PCI ASV workbench.

6. **Create an attestation** request draft. As you create the draft, you may need to do one or both of the following:

   - If your scan results include assets that are irrelevant to the attestation, **mark each irrelevant asset out of scope**.
   - If the scan results include any failures, create a **dispute** for each failure.

   **Note**: If you leave any failures undisputed when you submit your attestation for review, the ASV reviewer must fail the attestation.

7. After you have addressed all the failures, **submit the scan attestation for ASV review**.
Submit a Scan to the PCI ASV Workbench (Classic Interface)

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

After you create and launch your PCI ASV scan, you must import the scan to the PCI ASV scans table to start the review and attestation process.

Before you begin:

- [Create a scan](#) using the appropriate PCI ASV scan template. For information about PCI ASV scan templates, see [PCI ASV Scans (Classic Interface)](#).
- [Launch](#) the scan.

To submit a scan to the PCI ASV workbench:

1. In the top navigation bar, click **Scans**.

   The My Scans page appears.

2. In the **My Scans** table, click the scan you want to submit to the PCI workbench.

   **Note:** You can import only a [PCI External Quarterly Scan](#) or a [PCI WAS Scan](#) to the PCI ASV dashboard.

   **Note:** You cannot submit a scan to the PCI ASV dashboard that is more than 90 days old.

   The scans details page appears.

3. Click **Submit for PCI**.

   A **Submit Scan for PCI Validation** window appears.

   **Note:** If Tenable.io detects any failures in the scan, a message appears recommending that you submit a clean scan. You can either click **Fix Failures**, discard your scan, and **create another scan** or you can continue with the existing scan and address the failures after you create your attestation.
4. Click **Continue**.

A **Scan Submitted for PCI Validation** message appears.

The scan appears in the **New Scan Results** tab in your **PCI ASV** workbench.

**What to do next:**

- [Create an attestation](#) for the scan.
Create an Attestation (Classic Interface)

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Required User Role: Administrator

After you submit a PCI ASV scan to the PCI ASV dashboard, you must create an attestation request draft.

Note: When you create an attestation request draft for a scan, you do not also submit the scan for ASV attestation. You must dispute all remaining failures and address all out of scope assets before you submit the attestation for ASV approval.

Caution: You cannot create an attestation for scans that are more than 90 days old.

To create an attestation request:

1. In Tenable.io, in the top navigation bar, click Dashboards.
   
   The Vulnerabilities workbench appears.

2. In the left navigation bar, click PCI ASV.
   
   The PCI ASV Attestation Requests page appears.

3. In the scans table, in the New Scan Results tab, select the check box next to the scan or scans for which you want to create an attestation.

4. In the upper-right corner of the page, click Start Attestation.
   
   The Attestation Details page appears.

1. In the scans table, select the check box next to the scan or scans for which you want to create an attestation.

2. In the upper-right corner of the page, click Start Attestation.
   
   The PCI ASV Attestation Request / New Attestation page appears.
3. In the Name box, type the name of the attestation as you want it to appear on the attestation request.

   **Note:** Tenable recommends that you type a name you can easily identify. After you submit the attestation request, you cannot change the name on the attestation.

4. (Optional) To assign the attestation to a different user, in the Owner drop-down box, select the user to whom you want to assign the attestation.

5. Click Save.

   Tenable.io saves the attestation draft in the In Remediation tab of the PCI ASV table.

   **Note:** You can return to a saved, unsubmitted attestation and configure the options until you submit the attestation for review.

What to do next:

- If the scan includes any assets that are irrelevant to the PCI ASV review, [mark each irrelevant asset out of scope](#).
- If the new attestation displays any failures in the Undisputed Failures tab, [create a dispute](#) for each failure.
Mark an Asset as Out of Scope (Classic Interface)

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

To mark an asset as out of scope:

1. Click **Dashboards > Workbenches > PCI ASV**.
   
   The **PCI ASV Attestation Requests** page appears.

2. On the **In Remediation** tab, select the attestation that has an asset you want to mark out of scope.
   
   The **General Information** page for the scan appears.

3. Click the **Assets** tab.

4. (Optional) To mark one asset as out of scope, the row for that, click the **Mark as Out of Scope** button.
   
   Tenable.io removes the asset from PCI ASV review scope.

5. (Optional) To mark multiple assets as out of scope, do the following:
   - Select the check box next to each asset you want to mark out of scope.
     
     In the upper-right corner, the **Out of Scope** button appears.
   - Click **Out of Scope**.
     
     Tenable.io removes the assets from PCI ASV review scope.

What to do next:

- If your attestation request includes any undisputed failures, [create a dispute for each failure](#).
- If your attestation request has no undisputed failures, [submit the attestation request for ASV review](#).
Disputes (Classic Interface)

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

When you create and launch a PCI ASV scan, the scan results may include findings you want to dispute before you submit the associated attestation for review. To address these findings, you can create a dispute to submit to the ASV reviewer.

After you create a dispute, you can edit, clone, or delete the dispute as needed.

- [Create a Dispute (Classic Interface)]
- [Clone a Dispute to an Attestation (Classic Interface)]
- [Edit a Dispute (Classic Interface)]
- [Delete a Dispute (Classic Interface)]
Create a Dispute (Classic Interface)

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role**: Administrator

When you run a PCI scan and the scan detects failures, you must dispute the failures before you can submit the associated attestation for ASV review.

Before you begin:

- Create an Attestation (Classic Interface) for the scan.
- If your attestation includes assets that are not in scope for the PCI ASV review, mark each irrelevant asset as out of scope.

To create a dispute:

1. In Tenable.io, in the top navigation bar, click **Dashboards**.
   
   The Vulnerabilities workbench appears.

2. In the left navigation bar, click **PCI ASV**.
   
   The PCI ASV Attestation Requests page appears.

3. On the **In Remediation** tab, select the scan that has a failure you want to dispute.
   
   The PCI ASV Attestation Request / New Attestation page for the scan appears

   **Note**: By default, the General Information tab opens.

4. Click the **Undisputed Failures** tab.

   A table displaying the undisputed failures found in the scan appears.

   **Tip**: In the upper right corner, in the All Plugins drop-down box, you can select a plugin ID to filter the list of failures by plugin.

5. Select the check box next to the undisputed failure or failures you want to dispute.
6. Click **New Dispute**.

   The **New Dispute** page appears.

   **Note**: By default, the **Dispute Detail** tab opens. To see more information about the failure, click the **Failures** tab.

7. In the **Name** box, type a name for the dispute.

   **Note**: By default, a concatenation of the IP address and plugin ID associated with the failure appears in the **Name** box.

8. (Optional) To assign the dispute to a different user, in the **Owner** drop-down box, select the user you to whom you want to assign the dispute.

9. In the **Reason** drop-down box, select the reason for the dispute. For details on each reason, see **Dispute Reasons**.

10. In the **Explanation** text box, type an explanation for the dispute.

   **Note**: You can click the plugin ID to get more information about the failure and use the information in your explanation.

11. (Optional) To add an external file as evidence to support your dispute, do the following:

    - In the **Evidence** section, click **Add File**.
      
      An explorer window appears.
    
      - Select the file you want to add to your dispute.

   **Note**: PCI ASV does not restrict the file types you add to a dispute. Additionally, when you upload a file as evidence, PCI ASV automatically saves the uploaded file to the dispute before you click **Save** or **Cancel**.

12. Click **Save**.

   Tenable.io saves your dispute to the attestation.
A **Dispute created successfully** notification momentarily appears.

Your dispute appears in the **Disputes** tab.
Edit a Dispute (Classic Interface)

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

To edit a dispute:

1. In Tenable.io, in the top navigation bar, click **Dashboards**.
   
   The **Vulnerabilities** workbench appears.

2. In the left navigation bar, click **PCI ASV**.
   
   The **PCI ASV Attestation Requests** page appears.

3. On the **In Remediation** tab, select the attestation that includes a dispute you want to edit.
   
   The information details page for the attestation appears.

4. Click the **Disputes** tab.
   
   A table of your disputes appears.

5. Click the row of the dispute you want to edit.
   
   The dispute details page appears.

   **Note:** By default, the **Dispute Detail** tab opens. To see more information about the failure, click the **Failures** tab.

6. Change any information you wish to edit.

7. Click **Save**.

   Tenable.io saves your edits to the dispute.
Clone a Dispute to an Attestation (Classic Interface)

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

You can clone a dispute and add it to an attestation that you previously submitted for ASV review.

**Note:** When you clone a dispute into an attestation, any other disputes attached to the same attestation are deleted.

To clone disputes for an attestation:

1. In Tenable.io, in the top navigation bar, click **Dashboards**.
   
   The **Vulnerabilities** workbench appears.

2. In the left navigation bar, click **PCI ASV**.
   
   The **PCI ASV Attestation Requests** page appears.

3. On the **In Remediation** tab, select the attestation for which you want to clone all disputes.
   
   The information details page for the attestation appears.

4. In the upper-right corner, click the **Clone Disputes** drop-down box.
   
   The drop-down box expands, listing your existing attestations.

   **Note:** Only attestations that you previously submitted for ASV validation appear in the drop-down box.

5. Select the attestation that you want to clone the dispute to.

   A **Clone Disputes** message window appears.

6. Click **Continue**.

   A **Disputes Cloned Successfully** message appears.

   Tenable.io clones the dispute into the attestation.
**Note:** Tenable does not automatically include any newly-added assets for the current quarter in the previous quarter’s cloned disputes. To include these assets, you must manually add them to a new or existing dispute.
Delete a Dispute (Classic Interface)

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

**Note:** You cannot delete a dispute after you submit the attestation associated to the dispute for ASV review.

To delete a dispute:

1. In Tenable.io, in the top navigation bar, click **Dashboards**.
   
   The **Vulnerabilities** workbench appears.

2. In the left navigation bar, click **PCI ASV**.
   
   The **PCI ASV Attestation Requests** page appears.

3. On the **In Remediation** tab, click the attestation that includes a dispute you want to delete.
   
   The information details page for the attestation appears.

4. Click the **Disputes** tab.
   
   The **Disputes** page appears.

5. Do one of the following:

   - To delete one dispute, in the row corresponding to the dispute you want to delete, click the ✗ button.
     
     Tenable.io deletes the dispute.

   - To delete multiple disputes simultaneously:
     a. Select the check box next to each dispute you want to delete.
     b. In the upper-right corner, click **Delete**.
     
     Tenable.io deletes the dispute.
Submit an Attestation for ASV Review (Classic Interface)

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

Before you begin:

- [Create an attestation](#) for the scan you want to submit for ASV review.
- (Optional) If your attestation includes assets that are not in scope for the PCI ASV review, [mark each irrelevant asset as out of scope](#).
- (Optional) If your attestation includes undisputed failures, [create a dispute](#) for each failure.

To submit an attestation for ASV review:

1. In Tenable.io, in the top navigation bar, click **Dashboards**.
   
   The Vulnerabilities workbench appears.
2. In the left navigation bar, click **PCI ASV**.
   
   The **PCI ASV Attestation Requests** page appears.
3. On the **In Remediation** tab, click the attestation you want to submit for ASV review.
   
   The attestation details page for the attestation appears.
4. (Optional) To update the name of the attestation, in the **Name** box, type the name as you want it to appear on the attestation.
5. (Optional) To update the owner of the attestation, in the **Owner** drop-down box, select the owner you want to assign to the attestation.
6. Click **Send to ASV Review**.

**Note:** If there are any undisputed failures in the attestation, a message appears recommending that you dispute the failures. Click **Dispute Failures** and [create a dispute](#) for each failure.
Caution: If you submit an attestation that has undisputed failures to ASV for review, the ASV reviewer must fail the attestation.

7. Click **Continue**.

The **Scan Attestation** page appears.

8. On the **Scan Attestation** page, configure the attestation information:
   1. In the **Contact Name** field, type a contact for the attestation.
   2. In the **Email** field, type an email for the attestation contact.
   3. In the **Phone** field, type a phone number for the attestation contact.
   4. In the **Job Title** field, type a job title for the attestation contact.
   5. In the **Company Name** field, type the company at which the attestation contact works.
   6. In the **Website URL** field, type the URL for the company's website.
   7. In the **Address Line 1** field, type the address of the company.
   8. (Optional) In the **Address Line 2** field, type any additional address information for the company, such as a Suite number or Floor number.
   9. In the **City** field, type the city in which the company is located.
   10. In the **State / Province / Region** field, type the state, province, or region in which the company is located.
   11. In the **Zip / Postal Code** field, type the zip code for the company's address.
   12. In the **Country** field, type the country in which the company is located.

9. In the **Attestation Agreement** section, carefully read the terms of the attestation agreement.

10. Click **Attest**.

   An **Attestation Successfully Submitted for ASV Review** message appears and the attestation appears under the **In Remediation** tab in your **PCI ASV Workbench**.
**Note:** Once your attestation moves to the **In Remediation** or **Attestations** tab, the attestation is read-only. You cannot make additional changes to the attestation unless an ASV reviewer initiates an information request.

**Tip:** After you create your first attestation, the **Scan Attestation** screen automatically populates the above fields with your previously entered information.

What to do next:

- If the ASV reviewer requests additional information about your disputed failures, respond to the requests. For more information, see [Respond to an ASV Review Information Request (Classic Interface)](Respond to an ASV Review Information Request (Classic Interface)).
Respond to an ASV Review Information Request (Classic Interface)

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

After you submit your PCI ASV attestation for ASV review, the ASV reviewer may ask for additional information about your disputed failures.

You can respond to the reviewer directly in the dispute.

**Before you begin:**

- [Submit your attestation for ASV review](#).

**To respond to an information request:**

1. In Tenable.io, in the top navigation bar, click **Dashboards**.
   
   The **Vulnerabilities** workbench appears.

2. In the left navigation bar, click **PCI ASV**.
   
   The **PCI ASV Attestation Requests** page appears.

3. Click the **In ASV Review** tab.
   
   A table of your attestation requests appears.

4. Locate the attestation that has an ⚪ icon next to the last modified date.

5. Click the attestation.
   
   The attestation details page appears.

6. Click the **Disputes** tab.
   
   A table of your disputes appears.

7. Click the dispute that has an ⚪ icon next to the last modified date.
The dispute details page appears.

8. In the **Explanation** section, view the question or comment the ASV reviewer submitted.

9. Do one of the following:

   - If you want to submit a text-based response to the ASV reviewer, in the **Explanation** section, in the text box, type your response.
   - If you want to add a file as evidence to support your dispute:
     
     a. In the **Evidence** section, click **Add File**.

     An explorer window appears.

     b. Select the file you want to add to your dispute.

     **Note**: Tenable.io does not restrict the file types you add to a dispute. Additionally, when you upload a file as evidence, Tenable.io automatically saves the file to the dispute before you click **Save** or **Cancel**.

     c. (Optional) To add more files to the dispute, repeat the previous step.

     **Note**: You can add as many files as you want to a dispute as long as the total file size does not exceed 10 GB.

10. Click **Save**.

    A **Dispute Successfully Submitted** notification momentarily appears.

    Tenable.io submits your response to the ASV reviewer.

    **Note**: You cannot edit or delete a response after you submit it to the ASV reviewer.

11. Repeat steps 7-10 for each dispute in the **Disputes** tab that has an ![icon] next to the last modified date.
Manage Scans

To manage your scans, you can perform the following actions.
Create a Vulnerability Management Scan

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

In Tenable.io, you can create discovery, assessment, and agent scans using scan templates. For general information about templates and settings, see Scan Templates and Settings.

When you create a scan, Tenable.io assigns you owner permissions for the scan.

**Tip:** To quickly target specific vulnerabilities that previous scans have identified on your assets, create a remediation scan.

**Note:** Tenable.io limits the number of scans you can create to 10,000 scans. Tenable recommends you re-use scheduled scans instead of creating new scans. This approach helps to avoid latency issues in the user interface.

**Note:** PCI Quarterly External scan data is intentionally excluded from dashboards, reports, and workbenches. This is due to the scan's paranoid nature, which may lead to false positives that would otherwise not be detected. For more information, see PCI ASV Scanning Overview.

**Note:** You cannot apply more than 300,000 IP address targets to a scan.

Before you begin:

- If you want to create a scan from a user-defined template, create a user-defined template as described in Create a User-Defined Template.

- Create an access group for any targets you want to use in the scan and assign Can Scan permissions to the appropriate users.

To create a scan:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, in the Vulnerability Management section, click Scans.

   The Scans page appears.
3. In the upper-right corner of the page, click **Create a Scan**.

The **Select a Scan Template** page appears.

4. Click the **Scanner, Agent, or User Defined** tab to view available templates for your scan.

The tab appears.

**Note:** Users with Scan Operator permissions can see and use only the user-defined templates that are shared with their account.

**Tip:** For information about creating **Web Application** scans, see **Create a WAS Scan**.

5. Click the tile for the template you want to use for your scan.

The **Create a Scan** page appears.

6. Configure the scan:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Settings</strong></td>
<td>Configure the settings available in the scan template.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Basic Settings in Vulnerability Management Scans</strong> — Specifies the organizational and</td>
</tr>
<tr>
<td></td>
<td>security-related aspects of a scan template. This includes specifying the name of the scan,</td>
</tr>
<tr>
<td></td>
<td>its targets, whether you want to schedule the scan, and who has permissions for the scan.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Discovery Settings in Vulnerability Management Scans</strong> — Specifies how a scan performs</td>
</tr>
<tr>
<td></td>
<td>discovery and port scanning.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Assessment Settings in Vulnerability Management Scans</strong> — Specifies how a scan identifies</td>
</tr>
<tr>
<td></td>
<td>vulnerabilities, as well as what vulnerabilities are identified. This includes identifying</td>
</tr>
<tr>
<td></td>
<td>malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility</td>
</tr>
<tr>
<td></td>
<td>of web applications.</td>
</tr>
</tbody>
</table>
- **Report Settings in Vulnerability Management Scans** – Specifies whether the scan generates a report.
- **Advanced Settings in Vulnerability Management Scans** – Specifies advanced controls for scan efficiency.

### Credentials
Specify credentials you want Tenable.io to use to perform a credentialsed scan.

### Compliance/SCAP
Specify the platforms you want to audit. Tenable, Inc. provides best practice audits for each platform. Additionally, you can upload a custom audit file.

### Plugins
Select security checks by plugin family or individual plugin.

7. Do one of the following:

- If you want to save without launching the scan, click **Save**.
  
  Tenable.io saves the scan.

- If you want to save and launch the scan immediately, click **Save & Launch**.

  **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

  Tenable.io saves and launches the scan.
Edit a Vulnerability Management Scan Configuration

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can Configure

To edit a scan configuration:

1. In the upper-left corner, click the  button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Vulnerability Management** section, click **Scans**.

   The **Scans** page appears.

3. For Vulnerability Management scans, in the **Folders** section, click a folder to load the scans you want to view.

   The scans table updates to display the scans in the folder you selected.

4. (Optional) Search for the scan you want to edit. For more information, see **Tenable.io Tables**.

5. In the scans table, click the scan you want to edit.

   The scan details appear.

6. Click the  button next to the scan name.

   The **Update a Scan** page appears.

7. Change the scan configuration:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Settings</strong></td>
<td>Configure the settings available in the scan template.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Basic Settings in Vulnerability Management Scans</strong> – Specifies the organizational and security-related aspects of a scan template. This includes specifying the name of the</td>
</tr>
</tbody>
</table>
scan, its targets, whether you want to schedule the scan, and who has permissions for the scan.

- **Discovery Settings in Vulnerability Management Scans** — Specifies how a scan performs discovery and port scanning.

- **Assessment Settings in Vulnerability Management Scans** — Specifies how a scan identifies vulnerabilities, as well as what vulnerabilities are identified. This includes identifying malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility of web applications.

- **Report Settings in Vulnerability Management Scans** — Specifies whether the scan generates a report.

- **Advanced Settings in Vulnerability Management Scans** — Specifies advanced controls for scan efficiency.

<table>
<thead>
<tr>
<th>Credentials</th>
<th>Specify credentials you want Tenable.io to use to perform a credentialed scan.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance/SCAP</td>
<td>Specify the platforms you want to audit. Tenable, Inc. provides best practice audits for each platform. Additionally, you can upload a custom audit file.</td>
</tr>
<tr>
<td>Plugins</td>
<td>Select security checks by plugin family or individual plugin.</td>
</tr>
</tbody>
</table>

8. Do one of the following:

- If you want to save without launching the scan, click **Save**.
  
  Tenable.io saves the scan.

- If you want to save and launch the scan immediately, click **Save & Launch**.
**Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

Tenable.io saves and launches the scan.
Create a WAS Scan

**Required Additional License:** Tenable.io Web Application Scanning

**Required Tenable.io Web Application Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

To create a scan in the new Tenable.io Web Application Scanning interface:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, in the **Web App Scanning** section, click **Scans**.
   
   The Web Application Scanning **Scans** page appears.

   **Note:** If your Tenable.io Web Application Scanning license expires, your web application scans no longer appear in the scans table.

3. In the upper-right corner of the page, click the **Create Scan** button.
   
   The **Select a Scan Template** page appears. By default, the **Web Application** tab is active.

   **Tip:** For information about creating Vulnerability Management scans, see [Create a Vulnerability Management Scan](#).

4. Do one of the following:

   - To create a scan based on a **Tenable-provided scan template**, click the tile for the scan template you want to use for your scan.
     
     The **Create a Scan** page appears.

   - To create a scan based on a **user-defined scan template**:
     
     a. Click the **User Defined** tab.
     
     A list of user-defined scan templates appears.
b. Click the tile for the scan template you want to use for your scan.

The **Create a Scan** page appears.

**Note:** Tenable recommends that you run an **Overview** scan the first time you scan a target to determine which URL targets Tenable.io Web Application Scanning scans by default. Based on the results, you can run a scan via the **Scan** template and adjust the configurations to exclude certain targets.

**Note:** Users with **Scan Operator** permissions can see and use only the user-defined scan templates that are shared with their account. For more information, see [User Roles](#).

5. **Configure the scan:**

<table>
<thead>
<tr>
<th>Tab</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Settings</strong></td>
<td>Specifies the basic organizational and security-related aspects of a scan template. This includes specifying the name of the scan, the target, whether you want to schedule the scan, scan notifications, and who has permissions to view or modify the scan.</td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td>Specifies the URLs and file types you want included in or excluded from your scan.</td>
</tr>
<tr>
<td><strong>Assessment</strong></td>
<td>Specifies how a scan identifies vulnerabilities, as well as what vulnerabilities are identified. This includes identifying malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility of web applications.</td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td>Specifies advanced controls for scan efficiency.</td>
</tr>
<tr>
<td><strong>Credentials</strong></td>
<td>Specify the credentials you want Tenable.io Web Application Scanning to use to perform a credentialed scan.</td>
</tr>
<tr>
<td><strong>Plugins</strong></td>
<td>Select security checks by plugin family or individual plugin.</td>
</tr>
</tbody>
</table>

6. Do one of the following:

- If you want to save without launching the scan, click **Save**.

  Tenable.io Web Application Scanning saves the scan.
• If you want to save and launch the scan immediately, click **Save & Launch**.

Tenable.io Web Application Scanning saves and launches the scan.

**Note**: When you launch a scan, the time the scanner takes to complete the scan varies depending on the system load. To prevent unnecessarily lengthy scan times, avoid launching an excessive number of scans simultaneously.

Excessive numbers of concurrent scans may exhaust the system’s scanning capacity. If necessary, Tenable.io Web Application Scanning automatically staggers concurrent scans to ensure consistent scanning performance.

**Note**: Tenable.io Web Application Scanning aborts scans that remain in **pending** status for more than four hours. If Tenable.io Web Application Scanning aborts a scan, modify your scan schedules to reduce the number of overlapping scans. If you still have issues, contact Tenable Support.
Edit WAS Scan Settings

**Required Additional License:** Tenable.io Web Application Scanning

**Required Tenable.io Web Application Scanning User Role:** Scan Manager or Administrator

**Required Scan Permissions:** Can Configure

**Note:** This topic describes how to configure scan settings in the new interface only. If you activate the new interface, you can view a snapshot of your historical scan configurations in the classic interface, but you cannot modify configurations for scans run using any scan template other than the PCI WAS Scan template from the classic interface. For more information, see [Interface Activation Modes in WAS](#).

The settings you can configure in a web application scan or user-defined scan template depend on the Tenable-provided scan template type. For more information, see [Scan Templates](#).

To configure scan settings in the new interface:

1. In the upper-left corner, click the **button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Web App Scanning** section, click **Scans**.

   The Web Application Scanning **Scans** page appears.

   **Note:** If your Tenable.io Web Application Scanning license expires, your web application scans no longer appear in the scans table.

3. In the scans table, roll over the scan you want to configure.

   The action buttons appear in the row.

4. Click the ** button.

   The **Update a Scan** page appears.

5. Modify the scan settings.
6. Click **Save**.

Tenable.io saves the scan settings.
Set WAS Scan Permissions

**Required Additional License:** Tenable.io Web Application Scanning

**Required User Role:** Administrator

In an existing scan, you can add new user or group permissions or update existing permissions.

To add permissions in the new interface:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, in the **Web App Scanning** section, click **Scans**.
   
   The Web Application Scanning **Scans** page appears.

   **Note:** If your Tenable.io Web Application Scanning license expires, your web application scans no longer appear in the scans table.

3. In the scans table, hover over the row for the scan for which you want to set permissions.

4. On the right side of the row, click the button.
   
   The **Update a Scan** page appears.

5. In the **User Permissions** section, click the button.
   
   The **Add User Permission** plane appears.

6. In the **Add Users or Groups** drop-down box, select user name or group with whom you want to share the scan.

   The user name or group appears in the list of users below the drop-down box.

   **Tip:** If you are typing the name of the user name or group in the drop-down box, Tenable.io Web Application Scanning displays a list of options that match your text.

7. Next to the user or group name, in the drop-down box, select the permissions you want to apply to the user or group.
8. Click **Add**.

The **Add User Permission** plane disappears.

The user or group name appears under the **User Permissions** section, along with the permissions you selected.

9. Click **Save**.

Tenable.io Web Application Scanning updates the scan permissions.

To update existing permissions in the new interface:

**Note:** You cannot update permissions for the user that owns the scan.

1. In the upper-left corner, click the **Ξ** button.

The left navigation plane appears.

2. In the left navigation plane, in the **Web App Scanning** section, click **Scans**.

The Web Application Scanning **Scans** page appears.

**Note:** If your Tenable.io Web Application Scanning license expires, your web application scans no longer appear in the scans table.

3. In the scans table, hover over the row corresponding to the scan for which you want to set permissions.

4. On the right side of the row, click the **✏️** button.

The **Update a Scan** page appears.

5. In the **User Permissions** section, you can:

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update permissions for a user or group</td>
<td>In the drop-down box next to the user or group name, select the permissions you want to apply.</td>
</tr>
<tr>
<td>Remove all permissions from a user or group</td>
<td>• Roll over the user or group name.</td>
</tr>
</tbody>
</table>
A button appears next to the drop-down box.

- Click the button.

The user or group name disappears from the list.

6. Click **Save**.

Tenable.io Web Application Scanning updates the permissions.
Copy a Scan Configuration

**Required Tenable.io Vulnerability Management User Role:** Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Owner

When you copy a scan configuration, Tenable.io assigns you owner permissions for the copy and assigns the copy scan permissions from the original scan.

**Note:** You cannot copy a scan from the Remediation Scans folder.

To copy a scan configuration in the new interface:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. Do one of the following:

   • In the left navigation plane, in the **Vulnerability Management** section, click **Scans**.

   The Scans page appears.

   • In the left navigation plane, in the **Web App Scanning** section, click **Scans**.

   The Web Application Scanning Scans page appears.

   **Note:** If your Tenable.io Web Application Scanning license expires, your web application scans no longer appear in the scans table.

3. For Vulnerability Management scans, in the **Folders** section, click a folder to load the scans you want to view.

   The scans table updates to display the scans in the folder you selected.

4. In the scans table, roll over the scan you want to copy.

   The action buttons appear in the row.

   **Tip:** If 5 or more actions are possible, the button appears in the row. For more information, see Navigate a Table.
5. Do one of the following:

   - Vulnerability Management scans —
     a. In the row, click the button.
        A drop-down box of options appears.
     b. In the row, click the button.
        A drop-down box of options appears.
     c. Click Copy.
        The Copy to Folder plane appears, which contains a list of your scan folders.
     d. Click the folder where you want to save the copy.
     e. Click Copy.
        Tenable.io creates a copy of the scan with Copy of prepended to the name and assigns you owner permissions for the copy. The copy appears in the scans table of the folder you selected.

   - Web application scans —
     a. In the row, click the button.
        Tenable.io creates a copy of the scan with Copy of prepended to the name and assigns you owner permissions for the copy. The copy appears in the scans table.
Change Scan Ownership

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Manager or Administrator

**Required Scan Permissions:** Owner

Before you begin:

- If the scan is based on a [user-defined template](#), assign the new owner at least [Can View permissions](#) for that template. Otherwise, the new owner cannot view the scan configuration.

**Note:** Only the scan owner can change scan ownership. Therefore, if an administrator needs to change the ownership of another user's scan, they must first [assist](#) the user with their account and then assign ownership to the appropriate user.

To change the ownership of a scan in the new interface:

1. Edit a [Vulnerability Management](#) or [WAS](#) scan configuration.

2. In the left navigation menu, in the **Settings** section, click **Basic**.

   The **Basic** settings appear.

3. In the **User Permissions** section, next to the permission drop-down for **Owner**, click the ▼ button.

   A list of available user accounts appears.

4. Select a user from the list.

   Tenable.io automatically adds you to the list of users and assigns [Can View](#) permissions to your user account.

5. (Optional) Remove all permissions for your user account:

   a. In the user list, roll over your user account.

   The ✘ button appears at the end of the listing.
b. Click the \( \times \) button.

Tenable.io removes your account from the list of users.

6. (Optional) Edit the **Vulnerability Management permissions** or the **WAS permissions** for your user account:
   a. Next to the permission drop-down for your user account, click the \( \triangledown \) button.
   b. Select a permission.

7. Click **Save**.

Tenable assigns ownership to the selected user and assigns your user account the permissions you selected. If you removed all permissions for your user account from the scan, the scan no longer appears in any of your scan folders.
Organize Scans by Folder

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

In Tenable.io, the *Scans* page contains a *Folders* section that automatically groups your configured and imported scans into default folders. To further organize your scans, you can create custom folders.

To organize your scans by folder:

1. View scans in default folders.

   **Note:** You cannot rename or delete the default folders.

By default, Tenable.io provides the following folders:

<table>
<thead>
<tr>
<th>Folder</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>My Scans</strong></td>
<td>Contains scans that you have created or imported. This folder appears by default when you access the <em>Scans</em> page.</td>
</tr>
</tbody>
</table>
| **All Scans**| • (Administrators) Contains scans created by any users.  
|              | • (All other users) Contains:  
|              |   ◦ Scans that you have created  
|              |   ◦ Any shared scans for which you have *Can View* permissions or higher |
| **Remediation Scans** | Contains any *remediation scans* you own or that another user has shared with you. |
| **Trash**    | Contains scans that you have *moved* to the trash. If you have *Can Configure* permissions for a scan in this folder, you can permanently |
delete the scan for all users.

If you delete a custom folder that contains scans, Tenable.io automatically moves any scans in the deleted folder to the Trash folder.

Tenable.io automatically deletes Vulnerability Management scans stored in the Trash folder for longer than 30 days.

2. (Optional) Manage custom folders:
   - Create a custom folder.
   - Rename a custom folder.
   - Delete a custom folder.

   Note: The custom folders you create appear only to you and cannot be shared with other users.

3. Move a scan to the appropriate folder.

   From a default folder, you can move a scan to one of the following folders:
   - The My Scans default folder
   - A custom scan folder

   From a custom folder, you can move a scan to one of the following folders:
   - The My Scans default folder
   - A different custom folder

   Note: You cannot move scans to or from the Remediation Scans folder.
Create a Custom Scan Folder

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

The custom scan folders you create appear only to you and cannot be shared with other users. You are the only user who can view, rename, or delete the scan folders you create.

To create a scan folder:

1. In the upper-left corner, click the button.
   
The left navigation plane appears.

2. Do one of the following:
   
   • In the left navigation plane, in the Vulnerability Management section, click Scans.
     
The Scans page appears.
   
   • In the left navigation plane, in the Web App Scanning section, click Scans.
     
The Web Application Scanning Scans page appears.

   **Note:** If your Tenable.io Web Application Scanning license expires, your web application scans no longer appear in the scans table.

3. Next to Folders, click the button.
   
The New Folder box appears at the bottom of the folder list.

4. In the New Folder box, type a name for the folder.

5. Click the button.

   A Folder added successfully message appears and the new folder appears in the Folders section.
Move a Scan to a Scan Folder

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can View

You can move a scan from a default folder to either the My Scans default folder or a custom scan folder. You can also move a scan from a custom folder to the My Scans default folder or a different custom folder.

If you move a scan from the All Scans default folder, the scan appears in both the folder you select and the All Scans folder.

If you move a scan from the My Scans default folder, the scan appears in the custom folder only.

For information about moving a scan to the trash, see Move a Scan to the Trash Folder.

**Note:** You cannot move scans to or from the Remediation Scans folder.

To move a scan to a scan folder:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. Do one of the following:

   - In the left navigation plane, in the Vulnerability Management section, click Scans.

     The Scans page appears.

   - In the left navigation plane, in the Web App Scanning section, click Scans.

     The Web Application Scanning Scans page appears.
3. For Vulnerability Management scans, in the Folders section, click a folder to load the scans you want to view.

The scans table updates to display the scans in the folder you selected.

4. In the scans table, roll over the scan you want to move.

The action buttons appear in the row.

5. Do one of the following:
   - Vulnerability Management scans —
     a. In the row, click the button.

     A menu appears.

     b. In the menu, click Move.

     The Move to Folder plane appears. This plane contains a list of your scan folders.

   - Web application scans —
     a. In the row, click the button.

     The Move to Folder plane appears. This plane contains a list of your scan folders.

6. Search for a folder:
   a. In the search box, type the folder name.
   
   b. Click the button.

   Tenable.io limits the list to folders that match your search.

7. In the folder list, click the folder where you want to move the scan.

8. Click Move.

Tenable.io moves the scan to the selected folder.
## Rename a Custom Scan Folder

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can rename custom scan folders only. You cannot rename the default scan folders.

Renaming a scan folder affects your user account only, because the custom folders you create appear only to you and cannot be shared with other users.

To rename a scan folder:

1. In the upper-left corner, click the **Collapse** button.

   The left navigation plane appears.

2. Do one of the following:

   - In the left navigation plane, in the **Vulnerability Management** section, click **Scans**.

     The **Scans** page appears.

   - In the left navigation plane, in the **Web App Scanning** section, click **Scans**.

     The Web Application Scanning **Scans** page appears.

   **Note:** If your Tenable.io Web Application Scanning license expires, your web application scans no longer appear in the scans table.

3. In the **Folders** section, roll over the folder you want to rename.

   The action buttons appear in the row.

4. In the row, click the **Edit** button.

   An editable box replaces the folder name.

5. In the box, type a new name for the folder.
6. Click the ✓ button.

Tenable.io updates the folder name and a **Folder updated successfully** message appears.
Delete a Custom Scan Folder

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can delete custom scan folders only. You cannot delete the default scan folders that Tenable.io provides (All Scans, My Scans, and Trash).

Deleting a scan folder affects your user account only, because the custom folders you create appear only to you and cannot be shared with other users.

If you delete a scan folder that contains scans, Tenable.io moves the scans to the Trash folder.

To delete a scan folder:

1. In the upper-left corner, click the ** button.

   The left navigation plane appears.

2. Do one of the following:
   - In the left navigation plane, in the **Vulnerability Management** section, click **Scans**.

     The **Scans** page appears.
   - In the left navigation plane, in the **Web App Scanning** section, click **Scans**.

     The Web Application Scanning **Scans** page appears.

**Note:** If your Tenable.io Web Application Scanning license expires, your web application scans no longer appear in the scans table.

3. In the **Folders** section, roll over the folder you want to delete.

   The action buttons appear in the row.

4. In the row, click the ** button.

   A confirmation window appears.

5. Click **Delete** to confirm the action.

   A **Folder deleted successfully** message appears, and Tenable.io deletes the folder.
Move a Scan to the Trash Folder

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can View

When you move a shared scan to the Trash folder, Tenable.io moves the scan for your account only. The scan remains in the original folder for all other users who have Can View permissions or higher for the scan.

Scans moved to the Trash folder also appear in the All Scans folder, marked with the label, Trash.

**Note:** After you move a scan to the Trash folder, the scan remains in the Trash folder until a user with Can Configure permissions permanently deletes the scan.

**Note:** Scheduled scans do not run if they are in the scan owner’s Trash folder.

**Note:** You cannot move scans from the Remediation Scans folder to the Trash folder. Instead, delete remediation scans directly in the folder.

To move a scan or scans to the Trash folder:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. Do one of the following:
   - In the left navigation plane, in the Vulnerability Management section, click Scans.

     The Scans page appears.

   - In the left navigation plane, in the Web App Scanning section, click Scans.

     The Web Application Scanning Scans page appears.
Note: If your Tenable.io Web Application Scanning license expires, your web application scans no longer appear in the scans table.

3. In the **Folders** section, click the folder that contains the scan you want to move.

   The scans table lists scans in the selected folder.

4. Do one of the following:

   - **Select a single scan:**
     
     a. In the scans table, roll over the scan you want to move.

     The action buttons appear in the row.

     b. Click the button.

     A menu appears.

     c. Click Trash.

   - **Select multiple scans:**
     
     a. In the scans table, select the check box next to each scan you want to move.

     The action bar appears at the bottom of the page.

     b. In the action bar, click Trash.

   Tenable.io moves the scan or scans you selected to the **Trash** folder.
Delete a Scan

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can Configure

When you permanently delete a scan, you delete the scan configuration and scan results for all users the scan is shared with.

**Note:** The workflow for deleting a remediation scan differs from the workflow described in this procedure. For more information, see Delete a Remediation Scan.

**Caution:** After you delete a scan, you cannot recover the scan or any scan data associated with the scan. Delete only scans you are certain you no longer need to view or run.

Before you begin:

- If the scan you want to delete is a Vulnerability Management scan, move the scan to the Trash folder.

To delete a scan:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. Do one of the following:

   - In the left navigation plane, in the Vulnerability Management section, click Scans.
     
     The Scans page appears.

   - In the left navigation plane, in the Web App Scanning section, click Scans.

     The Web Application Scanning Scans page appears.
Note: If your Tenable.io Web Application Scanning license expires, your web application scans no longer appear in the scans table.

3. For a Vulnerability Management scan, in the **Folders** section, click the **Trash** folder.

   The scan table updates to display the scans in the trash folder.

4. Do one of the following:

   - **Select a single scan:**
     a. In the scans table, roll over the scan you want to delete.

        The action buttons appear in the row.

     b. In the row, click the ✗ button.

        A confirmation window appears.

   - **Select multiple scans:**
     a. In the scans table, select the check box next to the scans you want to delete.

        The action bar appears at the bottom of the page.

     b. In the action bar, click the ✗ button.

        A confirmation window appears.

5. In the confirmation window, click **Delete**.

   Tenable.io deletes the scan or scans you selected.
Delete a Remediation Scan

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can Configure

When you delete a remediation scan, you delete the scan configuration and scan results for all users the scan is shared with.

**Note:** Tenable.io deletes scan results older than 90 days.

To delete a remediation scan:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Vulnerability Management** section, click Scans.

   The Scans page appears.

3. In the **Folders** section, click the **Remediation Scans** folder.

   The scan table updates to display remediation scans that you own or that other users have shared with you. By default, the rows are sorted by **Created Date**.

4. Do one of the following:

   - **Select a single scan**:
     
     a. In the scans table, roll over the scan you want to delete.

        The action buttons appear in the row.

     b. In the row, click the button.

        A confirmation window appears.

   - **Select multiple scans**:
a. In the scans table, select the check box next to the scans you want to delete.

The action bar appears at the bottom of the page.

b. In the action bar, click the button.

A confirmation window appears.

5. In the confirmation window, click **Delete**.

Tenable.io deletes the scan or scans you selected.

**Note:** Tenable.io keeps up to 10,000 of the most recent remediation scan results. Once you have more than 10,000 remediation scan results, Tenable.io deletes the scan results, starting with the oldest result.
View Scans

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can View

Tenable.io defines *Archived* as any individual scan results that are older than 35 days. For scan results that are younger than 35 days, you can view and export the results in Tenable.io. For archived scan results, you can export the results, but cannot view them in Tenable.io. This limitation applies to both imported scan results and scan results that Tenable.io collects directly from scanners. After 15 months, Tenable.io removes the scan data entirely.

You can view configured and imported scans. If you have appropriate permissions, you can also perform actions to manage the scans.

Before you begin:

- Create or import one or more scans.

To view scans:

1. In the upper-left corner, click the menu button. The left navigation plane appears.

2. Do one of the following:
   - In the left navigation plane, in the *Vulnerability Management* section, click **Scans**. The **Scans** page appears.
   - In the left navigation plane, in the *Web App Scanning* section, click **Scans**. The Web Application Scanning **Scans** page appears.
3. For Vulnerability Management scans, in the **Folders** section, click a folder to load the scans you want to view.

   The scans table updates to display the scans in the folder you selected.

   For more information about scan folders, see [Organize Scans by Folder](#).

4. Do any of the following:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search box</td>
<td>Search the table by scan name or <strong>status</strong>. For more information, see <a href="#">Tenable.io Tables</a>.</td>
</tr>
</tbody>
</table>
   | Filter (Vulnerability Management, **All Scans** only) | To filter the **All Scans** folder by scan **status**:
   |                              | 1. Next to **Filters**, click the **button.** |
   |                              | The filter settings appear.                                           |
   |                              | 2. In the **Match** drop-down box, select one of the following:       |
   |                              |  \* **Match Any** – View results that match any of the filters you create. |
   |                              |  \* **Match All** – View results that match all of the filters you create. |
   |                              | 3. In the **Select Category** drop-down box, select **Status**.        |
   |                              | 4. In the **Select Operator** drop-down box, select **is equal to** or **is not equal to**. |
   |                              | 5. In the **Select Value** box, select the scan status by which you want to filter the **All Scans** table. |
   |                              | 6. (Optional) In the lower-left corner of the filter section:
   |                              |  \* To add another filter, click the **Add** button.                   |
| **Search box (web application scans only)** | **Filter** the table with Tenable-provided scan filters. |
| **Create Scan button** | In the upper-right corner, click the **Create Scan** button to create a new Vulnerability Management or web application scan. |
| **Tools button** | In the upper-right corner, click the **Tools** button. A menu appears with the following options: |
| | • Import Scan (Vulnerability Management scans only) |
| | • Manage Scan Templates |
| | • Manage Sensors |
| | • Manage Credentials |
| | • Manage Exclusions |
| **Scans table** | • View summary information about each scan: |
| | • **Name** — The scan name. |
| | If you have assigned permissions for the scan to other users, the label **Shared** appears next to the scan name. |
| | • **Schedule** — The scan schedule. |
| | • **Last Modified** — The date and time the scan was last modified. |
| | • **Status** — The [status](#) of the scan. |

7. Click **Apply**.

Tenable.io applies your filter or filters to the table.
• Sort, increase or decrease the number of rows per page, or navigate to another page of the table. For more information, see Tenable.io Tables.

• View details for a Vulnerability Management or web application scan.

• Change the read status for a scan.

• Export scan results.

• Move a scan to the trash.

• Delete a scan permanently.

• Move a scan to a different folder.
### WAS Scan Filters

On the **Scans** page, you can filter web application scans using Tenable-provided filters.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created Date</td>
<td>The date the scan configuration was created.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the scan configuration.</td>
</tr>
<tr>
<td>Finalized Date</td>
<td>The date on which the scan last completed.</td>
</tr>
<tr>
<td>Last Modified Date</td>
<td>The date on which the scan configuration was last modified.</td>
</tr>
<tr>
<td>Last Scanned Date</td>
<td>The date on which the scan was last ran.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the scan configuration.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Whether a scan schedule is enabled or on demand.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the scan. For more information about scan statuses, see <a href="#">Scan Status</a>.</td>
</tr>
<tr>
<td>Target</td>
<td>The target URL used to launch the scan.</td>
</tr>
<tr>
<td>Template</td>
<td>The Tenable-provided scan template the scan configuration was based on.</td>
</tr>
<tr>
<td>User Template</td>
<td>The user-defined scan template the scan configuration was based on.</td>
</tr>
</tbody>
</table>
View Vulnerability Management Scan Details

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can View

You can view scan results for scans you own and scans that were shared with you. Consider the following when viewing scan results:

- You can view details for an individual scan based on the permissions configured for the scan. However, when you view aggregated scan results in dashboards and other analysis views (for example, the Vulnerabilities or Assets tables), your access is based on the access groups you belong to.

- Tenable.io defines Archived as any individual scan results that are older than 35 days. For scan results that are younger than 35 days, you can view and export the results in Tenable.io. For archived scan results, you can export the results, but cannot view them in Tenable.io. This limitation applies to both imported scan results and scan results that Tenable.io collects directly from scanners. After 15 months, Tenable.io removes the scan data entirely.

- When you view results from the latest run of the scan, Tenable.io categorizes the scan as Read. The Read status is specific to your user account only. You can also manually change the read status.

- Tenable.io retains scan data for 15 months. If you want to store scan data for longer than 15 months, you can export the scan data for storage outside of Tenable.io.

To view scan results for an individual scan:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, in the Vulnerability Management section, click Scans.

   The Scans page appears.
3. For Vulnerability Management scans, in the **Folders** section, click a folder to load the scans you want to view.

The scans table updates to display the scans in the folder you selected.

4. In the scans table, click the scan where you want to view details.

The **Scan Details** page appears. By default, this page displays details for the latest run of the scan.

5. Do any of the following:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table header</td>
<td>• <strong>Export</strong> the scan results that Tenable.io is currently displaying.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit</strong> the scan configuration.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Move a scan to the trash</strong> folder.</td>
</tr>
<tr>
<td>Severity summaries</td>
<td>The number of vulnerabilities with a <strong>Critical</strong>, <strong>High</strong>, <strong>Medium</strong>, and <strong>Low severity</strong> in the scan results.</td>
</tr>
<tr>
<td><strong>Scan Details</strong> section</td>
<td>View details about the scan run:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Status</strong> – The <a href="#">status</a> of the scan.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Start Time</strong> – The start date and time for the scan.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Template</strong> – The <a href="#">Tenable-provided template</a> on which the scan configuration is based.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Scanner</strong> – The scanner that performed the scan.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Scanner Groups</strong> – The scanner group(s) to which Tenable.io assigned the scan. This detail appears only if <a href="#">scan routing</a> is enabled for the scan.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Targets</strong> – The targets that the scan evaluated.</td>
</tr>
</tbody>
</table>
### Vulns by Plugin tab

View the vulnerabilities in the scan results, organized by plugin.

**Note:** This tab does not appear for scan results older than 60 days.

- View information about each vulnerability:
  - **Severity icon** — The severity of the vulnerability.
  - **Name** — The name of the plugin that identified the vulnerability.
  - **Family** — The family of the plugin that identified the vulnerability.
  - **Vulnerabilities** — The number of vulnerability instances.

**Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

- To filter the data displayed in the table, see [Filter a Table](#).

- To sort, increase or decrease the number of rows per page, or navigate to another page of the table, see [Tenable.io Tables](#).

- To view details for a vulnerability, click a row of the table.

  The **Vulnerability Details** page appears. For more information, see [Vulnerability Details](#).

### Audit tab

View compliance audit check results. This tab only
appears if the scan results include data from compliance audit checks.

Tip: This tab does not appear for scan results older than 35 days.

On this tab, you can view:

- View tiles representing the number of audit checks identified the last time the scan completed, organized by severity level.
- View a table of audits detected during the scan. Each row represents a specific audit, and includes the following information:
  - **Status** — The status of the audit, for example Passed, Warning, or Failed.
  - **Name** — The name of the audit.
  - **Family** — The compliance check family to which the audit belongs.
  - **Count** — The number of times the audit was identified.
- To view additional information about a specific audit check, click a row in the audits table. The Audit Details page appears.
  - **Overview** — Information about the audit check, including a description of the check and the audit file used for the check.
  - **Assets** — A list of assets where the scan performed the audit check.
**Vulns by Asset** tab

View the vulnerabilities in the scan results, organized by asset. By default, assets in the table are sorted by decreasing number of vulnerabilities, then by decreasing severity.

**Tip:** This tab does not appear for scan results older than 35 days.

- View information about each vulnerability:
  - **Assets** – The asset identifier. Tenable.io assigns this identifier based on the presence of certain asset attributes in the following order:
    - Agent Name (if agent-scanned)
    - NetBIOS Name
    - FQDN
    - IPv4 address
  
  For example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the Asset Name.

  - **Vulnerabilities** – A visual summary of the vulnerabilities on the asset, organized by severity.

  - **Vuln Count** – The total number of vulnerabilities on the asset.

  - **Critical** – The total number of vulnerabilities on the asset with a critical severity.

  - **High** – The total number of vulnerabilities
on the asset with a high severity.

- **Audits** – A visual summary of the audits on the vulnerability, organized by severity.

- **Audit Count** – The total number of audits on the asset.

To filter the data displayed in the table, see [Filter a Table](#).

To sort, increase or decrease the number of rows per page, or navigate to another page of the table, see [Tenable.io Tables](#).

To view details for an asset, click a row of the table.

The **Asset Details** page appears. For more information, see [Asset Details](#).

### Warnings tab

View warnings about problems Tenable.io or the scanner encountered while running the scan. This tab only appears if Tenable.io or the scanner encountered an issue while running the scan.

Review the warnings to determine how to resolve the scan problem. For example, if an **Invalid Target** note is present, check the target parameters in the scan configuration.

**Tip:** This tab does not appear for scan results older than 35 days.

### Remediations tab

View remediation details.

**Note:** The **Remediation** tab only appears if there are known remediations for the scan.
This tab contains a table listing each remediation action. On this tab, you can view:

- **Vulnerabilities** – The number of vulnerabilities resolved by the recommended remediation.
- **Assets** – The number of assets scanned.

For more information, see [Launch a Remediation Scan](#).

### History tab

View the scan history.

This tab contains a table listing each time the scan has run. For the scan run currently displaying in the [Scan Details](#) page, Tenable.io adds the label **Current** to the run. By default, the latest scan run is labeled **Current**.

**Note:** Scan history is unavailable for imported scans and for configured scans that have not yet run.

On this tab, you can:

- View summary information about each time the scan was run:
  - **Start Time** – The start date and time for the scan.
  - **End Time** – The end date and time for the scan.
  - **Duration** – The duration of the scan.
  - **Status** – The status of the scan.
- **Filter** the data displayed in the table.
- Sort, increase or decrease the number of rows per page, or navigate to another page of the...
table. For more information, see Tenable.io Tables.

- View details for a historical scan by clicking a row in the table.

  Tenable.io marks the run you selected as **Current** and updates the **Scan Details** section to show data for the selected run.

  If the historical scan results are younger than 35 days, Tenable.io also updates the tabs on the **Scan Details** page.

  If the historical scan results are older than 35 days, the additional tabs are absent from the **Scan Details** page. Use `export` instead to obtain the results.
View WAS Scan Details

**Required Additional License:** Tenable.io Web Application Scanning

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can View

*Note:* This topic describes the process for viewing scan results in the new interface only.

If you activate the new interface, you can view scan results as follows:

- For scans run based on historical scan configurations, view results in either interface.
- For scans run based on new scan configurations, view results in the new interface only.

You can view scan results for web application scans you own or that the scan owners have shared with you.

*Note:* After Tenable.io completes the scan, it can take up to 10 minutes for the scan results to appear in the dashboard.

To view scan details for an individual web application scan:

1. In the upper-left corner, click the  button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Web App Scanning** section, click **Scans**.

   The Web Application Scanning **Scans** page appears.

*Note:* If your Tenable.io Web Application Scanning license expires, your web application scans no longer appear in the scans table.

3. For Vulnerability Management scans, in the **Folders** section, click a folder to load the scans you want to view.

   The scans table updates to display the scans in the folder you selected.

4. In the scans table, click the scan where you want to view details.
The **Scan Details** page appears. By default, this page displays details of the latest run of the scan.

5. Do any of the following:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table header</td>
<td>- <strong>Edit</strong> the scan configuration.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Move</strong> a scan to the trash folder.</td>
</tr>
<tr>
<td>Severity summaries</td>
<td>For the scan job currently displayed, view the number of vulnerabilities with a <strong>Critical</strong>, <strong>High</strong>, <strong>Medium</strong>, or <strong>Low</strong> vulnerability severity.</td>
</tr>
<tr>
<td>Scan Details section</td>
<td>For the scan job currently displaying, view the following details:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Status</strong> – The <strong>status</strong> of the scan.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Start Time</strong> – The start date and time for the scan.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Template</strong> – The <strong>scan template</strong> you used to configure and run the scan.</td>
</tr>
<tr>
<td></td>
<td>- <strong>End Time</strong> – The end date and time for the scan.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Scanner</strong> – The scanner that performed the scan.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Target</strong> – The target the scan evaluated.</td>
</tr>
<tr>
<td>Vulns by Plugin tab</td>
<td>For the scan job currently displayed, view vulnerability data, organized by plugin. On this tab, you can:</td>
</tr>
<tr>
<td></td>
<td>- View information about each vulnerability:</td>
</tr>
<tr>
<td></td>
<td>- Severity icon – The severity of the vulnerability.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Name</strong> – The name of the vulnerability, as defined in the Common Vulnerabilities and Exposures (CVE) system.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Family</strong> – The plugin family.</td>
</tr>
</tbody>
</table>
- **Vulnerabilities** – The number of vulnerability instances.

  **Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by the vulnerable URL and the input used to identify the vulnerability.

- To sort, increase or decrease the number of rows per page, or navigate to another page of the table, see **Tenable.io Tables**.

- To view vulnerability details, click the row for that vulnerability.

  The **Vulnerability Details** page appears.

  From the **Vulnerabilities Details** page, you can view [plugin attachments](#) for more information about each plugin.

### Notes tab

For the scan job currently displayed, view the scan notes that Tenable.io Web Application Scanning generates to provide context about your scan's success and efficiency.

The **Notes** tab appears and displays scan notes only if the scanner identifies information during the scan that can help you configure your scan for more effective results.

On this tab, you can:

- View information about the scan notes:

  - **Severity** – Metric used to quantify how significant the finding is for the scan's performance, displayed as Critical, High, Medium, Low, or Info. For information about scan notes vulnerability metrics, see [Scan Notes Severity Details in WAS](#).

  - **Scan Notes** – Descriptive title for the scan note.

  - **Description** – Detailed information about the scan findings, along with troubleshooting advice and suggestions to improve your overall scan quality.

### History tab

View the scan history.
This tab contains a table listing each time the scan has run. For the scan run currently displaying in the **Scan Details** page, Tenable.io adds the label **Current** to the run. By default, the latest scan run is labeled **Current**.

**Note:** Scan history is unavailable for imported scans and for configured scans that have not yet run.

On this tab, you can:

- View summary information about each time the scan was run:
  - **Created At** – The start date and time the scan was created.
  - **Start Time** – The start date and time the scan was started by the scanner.
  - **End Time** – The end date and time the scan was completed.
  - **Duration** – The duration of the scan.

**Note:** The **Duration** time span includes the time Tenable.io Web Application Scanning takes to run the scan and process the results, as well as any time the scan spent in **Pending** status.

As a result, **Duration** time differs from the **Overall Max Scan Time** you specified in the **Advanced settings**, which applies only to the scan run time.

- **Status** – The status of the scan.
  - **Filter** the data displayed in the table.
  - Sort or navigate to another page of the table. For more information, see **Tenable.io Tables**.
  - View details for a historical scan by clicking a scan job row in the table.
Tenable.io Web Application Scanning marks the scan job you selected as **Current** and updates the **Scan Details** section to show data for the selected job.
Scan Notes Severity Details in WAS

Tenable.io Web Application Scanning uses the severity ratings described below to categorize scan notes that appear in your scan results.

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Information explaining that the scan may have impacted the web application's availability or integrity. The scan note title appears in red.</td>
<td><strong>Service Stopped Responding</strong> — The scanner aborted the scan after encountering too many consecutive request timeouts. The scan results may be incomplete, and you should verify that the target is not corrupted or unavailable. Tenable recommends that you investigate the repeated timeouts to determine why the target cannot support the requests the scanner sent. You may need to decrease performance configurations in the scan template.</td>
</tr>
<tr>
<td>High</td>
<td>Information explaining that the scan stopped unexpectedly before the scanner finished analyzing the web application targets. As a result, the scan did not sufficiently analyze the web application for vulnerabilities, and the user should troubleshoot and re-attempt the scan. The scan note title appears in yellow.</td>
<td><strong>Scan Crashed</strong> — The scan crashed for an unexpected reason. As a result, the scan results are be missing or incomplete.</td>
</tr>
<tr>
<td>Medium</td>
<td>Information explaining why scan results are missing or incomplete. The findings usually concern scans that could not be</td>
<td><strong>Out of Scope URL</strong> — The scanner did not scan the target URL because it matches one of the</td>
</tr>
<tr>
<td>Level</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td>Information explaining variations in scan duration. The findings do not impact the web application or scan results. The scan note title appears in green.</td>
<td></td>
</tr>
<tr>
<td><strong>Target Response Has Been Truncated</strong></td>
<td>The target scan results exceeded the <strong>Max Response Size</strong> specified in the scan configurations. As a result, the content is truncated, which could cause data collection and assessment errors.</td>
<td></td>
</tr>
<tr>
<td><strong>Info</strong></td>
<td>Information that does not impact the scan results, but that can help you configure your scan settings more efficiently. The scan note title appears in blue.</td>
<td></td>
</tr>
<tr>
<td><strong>Authentication Detected</strong></td>
<td>The scanner detected an HTTP server authentication or login form. You can configure your credentials to allow the scanner to access more pages.</td>
<td></td>
</tr>
</tbody>
</table>
Launch a Vulnerability Management Scan

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can Control

In addition to configuring Schedule settings for a scan, you can manually start a scan run.

You can launch the scan using the targets as configured in the scan, or you can launch the scan with custom targets that override the configured targets.

To launch a scan:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, in the Vulnerability Management section, click Scans.

   The Scans page appears.

3. For Vulnerability Management scans, in the Folders section, click a folder to load the scans you want to view.

   The scans table updates to display the scans in the folder you selected.

   For more information about scan folders, see Organize Scans by Folder.

4. In the scans table, roll over the scan you want to launch.

   The action buttons appear in the row.

5. Do one of the following:

   - To launch the scan using the targets as configured in the scan, click the button in the row.

   - If you have previously launched the scan and want to use custom targets that override the configured targets:
a. In the row, click the button.

The Custom Launch Scan plane opens.

b. In the Targets box, type a comma-delimited string of targets.

c. Click Launch.

Tenable.io launches the scan.
Launch a Remediation Scan

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Access Group Permissions:** Can Scan

You can create a remediation scan to run a follow-up scan against existing scan results. A remediation scan evaluates a specific plugin against a specific scan target or targets where a vulnerability was present in your earlier active scan.

Remediation scans allow you to validate whether your vulnerability remediation actions on the scan targets have been successful. If a remediation scan cannot identify a vulnerability on targets where the vulnerability was previously identified, the system changes the status of the vulnerability to **Fixed**.

You can perform remediation scans for scan results from certain sensors only:

<table>
<thead>
<tr>
<th>Sensor Type</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable.io cloud</td>
<td>yes</td>
</tr>
<tr>
<td>On-premises Nessus</td>
<td>yes</td>
</tr>
<tr>
<td>Nessus scanner for Amazon Web Services (AWS)</td>
<td>yes</td>
</tr>
<tr>
<td>On-premises Tenable.io Web Application Scanning</td>
<td>no</td>
</tr>
<tr>
<td>Nessus Network Monitor</td>
<td>no</td>
</tr>
<tr>
<td>Nessus Agent</td>
<td>no</td>
</tr>
</tbody>
</table>

To launch a remediation scan:
1. Set the scope for the remediation scan:

<table>
<thead>
<tr>
<th>Remediation Scan Scope</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>All vulnerabilities on all affected assets</td>
<td>This scope is not supported.</td>
</tr>
<tr>
<td>All vulnerabilities on an individual asset</td>
<td>To set this scope:</td>
</tr>
<tr>
<td></td>
<td>a. <a href="#">View</a> asset details.</td>
</tr>
<tr>
<td></td>
<td>b. On the Asset Details page, click the Vulnerabilities tab.</td>
</tr>
<tr>
<td></td>
<td>The Vulnerabilities tab appears.</td>
</tr>
<tr>
<td></td>
<td>c. In the upper-right corner, click the Actions button.</td>
</tr>
<tr>
<td></td>
<td>The actions menu appears.</td>
</tr>
<tr>
<td></td>
<td>d. In the actions menu, click <a href="#">Launch Remediation Scan</a>.</td>
</tr>
<tr>
<td>All vulnerabilities on multiple assets</td>
<td>This scope is not supported.</td>
</tr>
<tr>
<td>An individual vulnerability on the top 500 affected assets</td>
<td>To set this scope:</td>
</tr>
<tr>
<td></td>
<td>a. <a href="#">View</a> vulnerability details.</td>
</tr>
<tr>
<td></td>
<td>b. Click the Assets Affected tab.</td>
</tr>
<tr>
<td></td>
<td>The assets table appears.</td>
</tr>
<tr>
<td></td>
<td>c. In the upper-right corner, click the Actions button.</td>
</tr>
<tr>
<td></td>
<td>The actions menu appears.</td>
</tr>
<tr>
<td></td>
<td>d. Click <a href="#">Launch Remediation Scan</a>.</td>
</tr>
<tr>
<td>An individual vulnerability on an individual asset</td>
<td>To set this scope:</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td>a. View vulnerability details.</td>
</tr>
<tr>
<td></td>
<td>b. Click the Assets Affected tab.</td>
</tr>
<tr>
<td></td>
<td>The assets table appears.</td>
</tr>
<tr>
<td></td>
<td>c. In the assets table, select the check box for the asset you want to select.</td>
</tr>
<tr>
<td></td>
<td>The action bar appears at the bottom of the page.</td>
</tr>
<tr>
<td></td>
<td>d. In the action bar, click Launch Remediation Scan.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>An individual vulnerability on multiple assets</th>
<th>To set this scope:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a. View vulnerability details.</td>
</tr>
<tr>
<td></td>
<td>b. Click the Assets Affected tab.</td>
</tr>
<tr>
<td></td>
<td>The assets table appears.</td>
</tr>
<tr>
<td></td>
<td>c. In the assets table, select the check box next to each asset you want to select.</td>
</tr>
<tr>
<td></td>
<td>The action bar appears at the bottom of the page.</td>
</tr>
<tr>
<td></td>
<td>d. In the action bar, click Launch Remediation Scan.</td>
</tr>
</tbody>
</table>

| Multiple vulnerabilities on all affected assets | This scope is not supported. |

<table>
<thead>
<tr>
<th>Multiple vulnerabilities on an individual asset</th>
<th>To set this scope:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a. View asset details.</td>
</tr>
</tbody>
</table>
b. On the **Asset Details** page, click the **Vulnerabilities** tab.

The **Vulnerabilities** tab appears.

c. In the vulnerabilities table, select the check box next to each vulnerability you want to select.

The action bar appears at the bottom of the page.

d. In the action bar, click **Launch Remediation Scan**.

| Multiple vulnerabilities on multiple assets | This scope is not supported. |

The **Create a Scan - Remediation Scan** appears.

Tenable.io automatically creates the remediation scan from the Tenable-provided Advanced Network Scan template and populates certain settings based on the assets and vulnerabilities you selected.

2. On the **Create a Scan** page:

   a. Verify the settings that Tenable.io populated based on the vulnerabilities and assets you selected.

   b. Configure additional **settings** for the scan.

      The number of manual changes you must make depends on the plugins involved in the remediation scan.

The following table defines the inherited and default values for settings in the remediation scan.

<p>| Setting Category | Setting | Remediation Scan Value |</p>
<table>
<thead>
<tr>
<th>Basic</th>
<th>Name</th>
<th>Specifies an editable scan name in the format &quot;Remediation scan of plugin # number&quot; where number is the number of the plugin that identified the vulnerability.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder</td>
<td>Cannot be configured. Remediation scans appear in the Remediation Scans folder only.</td>
<td></td>
</tr>
<tr>
<td>Scanner</td>
<td>Specifies the scanner that performs the scan. The scanner you select depends on the location of the targets included in the remediation scan. For example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- By default, this value is the cloud scanner for your geographical region (for example, US Cloud Scanner). However, a cloud scanner cannot scan non-routable IP addresses. If the scan targets include non-routable IP addresses, select a linked scanner instead.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Select a scanner group if you want to:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Improve scan speed by balancing the scan load among multiple scanners.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Rebuild scanners and link new scanners in the future without having to update scanner designations in scan configurations.</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>(Required if the scanner is set to Auto-Select) Do one of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- If your scans involve separate environments with overlapping IP ranges, select</td>
<td></td>
</tr>
</tbody>
</table>
If your scans do not involve separate environments with overlapping IP ranges, retain the **Default** network.

<table>
<thead>
<tr>
<th><strong>Targets</strong></th>
<th>Specifies the scan targets based on the assets you selected for the remediation scan.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Permissions</strong></td>
<td>Specifies default settings for the Advanced Network Scan template. By default, only you have access to the individual scan results for the remediation scan. The <strong>Default</strong> user permissions are set to <strong>No Access</strong>. If you want to share the remediation scan with other users, configure the <strong>user permissions</strong>.</td>
</tr>
<tr>
<td><strong>Schedule</strong></td>
<td>Cannot be configured. If you do <em>not</em> launch a remediation scan when you create it, you can launch the scan manually later.</td>
</tr>
<tr>
<td><strong>all other settings</strong></td>
<td>Specifies default settings for the Advanced Network Scan template.</td>
</tr>
<tr>
<td><strong>Discovery</strong></td>
<td>all</td>
</tr>
<tr>
<td><strong>Assessment</strong></td>
<td>all</td>
</tr>
<tr>
<td><strong>Report</strong></td>
<td>all</td>
</tr>
</tbody>
</table>

**Note:** The default **Port Scan Range** scans common ports only. If the plugins used in the remediation scan require specific ports, configure this setting for a range that includes those ports.
### Scan Template Configuration

<table>
<thead>
<tr>
<th>Advanced</th>
<th>all</th>
<th>Specifies default settings for the Advanced Network Scan template.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credentials</td>
<td>all</td>
<td>By default, there are no credentials configured. If the plugins in the remediation scan require credentials, configure them in the remediation scan.</td>
</tr>
<tr>
<td>Compliance</td>
<td>all</td>
<td>By default, no compliance audits are configured. If the plugins in the remediation scan require compliance audit settings, configure the appropriate settings.</td>
</tr>
</tbody>
</table>
| Plugins | limited | Specifies plugins limited to the following:  
- the plugins you selected for remediation scanning  
- any plugins on which the selected plugins are dependent |

### 3. Do one of the following:

- If you want to save without launching the scan, click **Save**.  
  Tenable.io saves the scan.  
- If you want to save and launch the scan immediately, click **Save & Launch**.
Note: If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

Tenable.io saves and launches the scan.

What to do next:

- In the **Remediation Scans** folder on the **Scans** page:
  - **View** the scan status to determine when the scan completes.
  - **Edit** the scan configuration.
  - **Change** the read status of the scan results.
  - **Launch** the scan.

- Once the scan completes:
  1. On the **Vulnerabilities** page, **search** on the plugin.
  2. Verify that the status for the selected vulnerabilities is now **Fixed** on the assets that the remediation scan targeted.
Launch a WAS Scan

Required Additional License: Tenable.io Web Application Scanning

Required Tenable.io Web Application Scanning User Role: Scan Operator, Standard, Scan Manager, or Administrator

Required Scan Permissions: Can Control

**Note:** When you launch a scan, the time the scanner takes to complete the scan varies depending on the system load. To prevent unnecessarily lengthy scan times, avoid launching an excessive number of scans simultaneously.

Excessive numbers of concurrent scans may exhaust the system’s scanning capacity. If necessary, Tenable.io Web Application Scanning automatically staggers concurrent scans to ensure consistent scanning performance.

To launch a scan in the new interface:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Web App Scanning** section, click **Scans**.

   The Web Application Scanning **Scans** page appears.

   **Note:** If your Tenable.io Web Application Scanning license expires, your web application scans no longer appear in the scans table.

3. Do one of the following:

   * To launch a single scan:

     a. In the scans table, roll over the scan you want to launch.

     b. On the right side of the row, click the button.

     The scan launches and the **Status** column updates to reflect the status of the scan.
• To launch multiple scans:
  
a. In the scans table, select the check box(es) next to the scans you want to launch.

     The action bar appears at the bottom of the page.

b. In the action bar, click the ▶ button.

     The scans launch and the respective Status columns update to reflect the statuses of the scans.

4. **View** the scan progress.

5. As the scan progresses, monitor the **scan status**.

---

**Note:** Tenable.io Web Application Scanning aborts scans that remain in *pending* status for more than four hours. If Tenable.io Web Application Scanning aborts a scan, modify your scan schedules to reduce the number of overlapping scans. If you still have issues, contact Tenable Support.
# View WAS Scan Progress

**Required Additional License:** Tenable.io Web Application Scanning

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can Control

When you launch a web application scan, you can view the progress of the scan as it runs. Because scan progress information is based on historical data, Tenable.io Web Application Scanning scan progress data appears only for historical scans.

To view scan progress for a web application scan:

1. **Launch** an existing scan.
   
   The scan status appears in the **Status** column.

2. After the status changes from **Pending** to **Running**, next to the scan status, view the following scan progress indicators:

<table>
<thead>
<tr>
<th>Progress Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage</td>
<td>Portion of the scan job that the scanner has already completed, displayed as a percentage of the total estimated scan time.</td>
</tr>
<tr>
<td>Estimate</td>
<td>Estimated time remaining for the scanner to complete the scan, displayed in minutes.</td>
</tr>
<tr>
<td>Overdue</td>
<td>Amount of extra time the scan job is taking compared to previous scan jobs. This indicator only appears if the scan is running longer than previous scans.</td>
</tr>
<tr>
<td>Progress bar</td>
<td>Visual indicator of the time remaining for the scanner to complete the scan. When the scan is complete or stops for any other reason (for example, if Tenable.io aborts the scan), the progress bar disappears.</td>
</tr>
</tbody>
</table>
Pause or Resume a Scan

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can Control

You can pause scans that you want to temporarily stop. When you pause a scan, Tenable.io pauses all active tasks for that scan. The paused tasks continue to fill the task capacity of the scanner that the tasks were assigned to. Tenable.io does not dispatch new tasks from a paused scan job. If the scan remains in a paused state for more than 14 days, the scan times out. Tenable.io terminates the related tasks on the scanner and categorizes the scan as aborted.

You can resume scans that you previously paused. When you resume a scan, Tenable.io instructs the scanner to start the tasks from the point at which the scan was paused. If Tenable.io encounters problems when resuming the scan, the scan fails, and Tenable.io categorizes the scan as aborted.

To pause or resume a scan in the new interface:

1. In the upper-left corner, click the **Pause or Resume** button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Vulnerability Management** section, click **Scans**.

   The **Scans** page appears.

3. In the scans table, roll over the scan.

   The action buttons appear in the row.

4. Do one of the following:

   - To pause the scan, click the **Pause** button in the row.
   - To resume the scan, click the **Resume** button in the row.

   A confirmation window appears.

5. In the confirmation window, click **Pause** or **Resume** as appropriate.

   Tenable.io pauses or resumes the scan.
Stop a Running Scan

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can Control

When you stop a scan, Tenable.io terminates all tasks for the scan and categorizes the scan as canceled. The scan results associated with the scan reflect only the completed tasks. You cannot stop individual tasks, only the scan as a whole.

To stop a running scan:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. Do one of the following:
   
   - In the left navigation plane, in the **Vulnerability Management** section, click **Scans**.
     
     The **Scans** page appears.
   
   - In the left navigation plane, in the **Web App Scanning** section, click **Scans**.
     
     The Web Application Scanning **Scans** page appears.

   **Note:** If your Tenable.io Web Application Scanning license expires, your web application scans no longer appear in the scans table.

3. In the scans table, roll over the scan you want to stop.
   
   The action buttons appear in the row.

4. In the row, click the button.
   
   A confirmation window appears.
5. In the confirmation window, click **Stop**.

   Tenable.io stops the scan. The **Status** column updates to reflect the **status** of the scan.
Import a Scan

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can import scan results into Tenable.io. You cannot import results from scans run more than 15 months ago.

Imported scans always belong to the default network. For more information, see [Networks](#).

**Note:** Tenable.io supports scan imports up to 4GB in size.

To import a scan in the new interface:

1. In the upper-left corner, click the ☑️ button.
   
   The left navigation plane appears.

2. In the left navigation plane, in the **Vulnerability Management** section, click **Scans**.
   
   The **Scans** page appears.

3. In the upper-right corner of the page, click the [← Import] button.
   
   A file selection window appears.

4. Browse to and select the scan file you want to import.
   
   If the scan file is a .nessus or .db file, the **Import** plane appears.
   
   If the scan file is any other file type, the **Scan Import** window appears.

5. Do one of the following:
   
   - If the scan file is a .nessus or .db file:
     
     a. In the **Password** box, type the password to allow Tenable.io to view the scan.
     
     b. (Optional) To show the scan results in dashboards, select the **Show in Dashboard?** check box.
     
     c. Click **Import**.
If the scan file is any other file type, specify if you want the scan results to appear in dashboards:

- Click **Yes** to show the scan results in dashboards.
- Click **No** to prevent the scan results from appearing in dashboards.

*Note:* Clicking **Cancel** cancels the import.

The **Scans** page appears, and the imported scan appears in the scans table.

Tenable.io begins processing the imported scan results. Once this process is complete, the imported data appears in the individual scan details and aggregated data views (such as dashboards). This process can take up to 30 minutes, depending on the size of the import file.

**Tip:** If the imported data does not appear in the individual scan results or aggregated data views after a reasonable processing time, verify that you are assigned adequate permissions for the imported targets in **access groups**.
Delete a Scan Job

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can Configure

When you delete a scan job, you delete only the scan results for a single instance of the scan being launched, known as a scan job. After you delete a scan job, you can launch the same scan. You can also still view the results from previous scan jobs run using the scan configuration.

To delete a scan job or jobs:

1. In the upper-left corner, click the ☐️ button.
   
The left navigation plane appears.

2. Do one of the following:
   
   • **Vulnerability Management scan** –
     
     a. For Vulnerability Management scans, in the **Folders** section, click a folder to load the scans you want to view.
     
     The scans table updates to display the scans in the folder you selected.
   
   • **Web application scan** –
     
     a. In the left navigation plane, in the **Web App Scanning** section, click **Scans**.
     
     The Web Application Scanning **Scans** page appears.

   **Note:** If your Tenable.io Web Application Scanning license expires, your web application scans no longer appear in the scans table.

3. In the scans table, click the scan for which you want to delete a scan job.
   
The **Scan Details** page appears. By default, this page displays details of the latest scan job.
4. Click the **History** tab.

   The **History** tab appears, displaying a table listing each scan job previously run for the scan configuration.

5. Select the scan job or jobs you want to delete:

   - **Select a single scan job:**
     a. In the scan jobs table, roll over the scan job you want to delete.
        The action buttons appear in the row.
     b. In the row, click the 🗑 button.
        A confirmation window appears.

   - **Select multiple scan jobs:**
     a. In the scan jobs table, select the check box for each scan job you want to delete.
        The action bar appears at the bottom of the page.
     b. In the action bar, click the 🗑 button.
        A confirmation window appears.

6. In the confirmation window, click **Trash**.

   Tenable.io deletes the scan job or jobs you selected.
Change the Scan Read Status

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can View

On the **Scans** page, a scan appears in bold in the scans table if you have *not* yet viewed (read) the results of the latest run of the scan.

If you **view** the scan results, Tenable.io categorizes the scan as "read" and removes the bold formatting from the scan in the scans table.

You can also manually change the scan read status.

To change the scan read status:

1. **View** your scans.

2. In the scans table, roll over the scan you want to change.
   
   The action buttons appear in the row.

3. Click the ✉️ button.
   
   A menu appears.

4. Do one of the following:
   
   - If the scan has been read, click ✉️ **Mark Unread**.
   
   - If the scan has not been read, click ✉️ **Mark Read**.

   Tenable.io changes the read status for the scan.
Unarchive a Scan

Any individual scan results older than 35 days are categorized by Tenable.io as "archived." In Tenable.io, you can view and export scan results that are younger than 35 days. Archived scan results, however, can be exported, but not viewed.

**Note:** This limitation applies to both imported scan results and scan results that Tenable.io collects directly from scanners.

To view archived scan results in Tenable.io, you must unarchive results for individual scan results.

To unarchive a scan:

1. In the upper-left corner, click the ☰ button.
   
   The left navigation plane appears.

2. In the left navigation plane, in the **Vulnerability Management** section, click **Scans**.
   
   The **Scans** page appears.

3. In the scans table, click on the scan you want to unarchive.
   
   The **Scan Details** page appears.

4. In the **History** table, roll over the scan row.
   
   The action buttons appear in the row.

5. At the end of the row, click the ✉️ **Unarchive** button.

   Tenable.io unarchives the scan. View the scan in the scans table to see the unarchived scan.

**Note:** Tenable.io may take some time to unarchive a scan. Scan results can be exported while Tenable.io unarchives the scan, however the archive process must complete before you can view full scan data in Tenable.io.
Export Scan Results

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can View

You can export both imported scan results and results that Tenable.io collects directly from scanners.

Tenable.io retains individual scan results until the results are 15 months old.

---

**Note:** For archived scan results (that is, results older than 35 days), the export format is limited to `.nessus` and `.csv` files.

**Note:** When a scan is actively running, the Export button does not appear in the Tenable.io interface. Wait until the scan completes, then export the scan results.

---

To export results for an individual scan in the new interface:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. Do one of the following:

   - In the left navigation plane, in the **Vulnerability Management** section, click **Scans**.
     
     The **Scans** page appears.

   - In the left navigation plane, in the **Web App Scanning** section, click **Scans**.
     
     The Web Application Scanning **Scans** page appears.

---

**Note:** If your Tenable.io Web Application Scanning license expires, your web application scans no longer appear in the scans table.
3. For Vulnerability Management scans, in the **Folders** section, click a folder to load the scans you want to view.

   The scans table updates to display the scans in the folder you selected.

4. Do one of the following:

<table>
<thead>
<tr>
<th><strong>Location</strong></th>
<th><strong>Scope of Export</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Scans table</td>
<td>a. In the scans table, roll over the scan you want to export.</td>
</tr>
<tr>
<td></td>
<td>b. Click the : button.</td>
</tr>
<tr>
<td></td>
<td>A menu appears.</td>
</tr>
<tr>
<td></td>
<td>c. Click <strong>Export</strong>.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Export</strong> plane appears.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Scan Details</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a. In the scans table, click the scan you want to export.</td>
</tr>
<tr>
<td></td>
<td>b. Next to the scan name, click <strong>Export</strong>.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Export</strong> plane appears.</td>
</tr>
</tbody>
</table>

5. Select an export format:

<table>
<thead>
<tr>
<th><strong>Format</strong></th>
<th><strong>Description</strong></th>
<th><strong>Supported for Archived Scan Results</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerability Management Scans</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PDF - Custom</td>
<td>An Adobe .pdf file.</td>
<td>No</td>
</tr>
<tr>
<td><strong>Note:</strong> Tenable.io cannot export PDF files with more than 400,000 individual scan results.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PDF - Executive Summary</td>
<td>An Adobe .pdf file.</td>
<td>No</td>
</tr>
<tr>
<td><strong>Note:</strong> Tenable.io cannot export PDF files with more than</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report Type</td>
<td>Format Description</td>
<td>Exportable</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>HTML - Custom</td>
<td>A web-based .html file.</td>
<td>No</td>
</tr>
<tr>
<td>HTML - Executive Summary</td>
<td>A web-based .html file.</td>
<td>No</td>
</tr>
<tr>
<td>Nessus</td>
<td>A .nessus file in XML format that contains the list of targets, scan settings defined by the user, and scan results. Password credentials are stripped so they are not exported as plain text in the XML. If you import a .nessus file as a user-defined scan template, you must re-apply your passwords to any credentials.</td>
<td>Yes</td>
</tr>
<tr>
<td>CSV</td>
<td>A .csv text file with only scan results.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Note:
When exporting scan results as a .csv file, the severities always display CVSSv2 scores regardless of your configured severity metric.

#### Web Application Scans

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Format Description</th>
<th>Exportable</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTML</td>
<td>A web-based .html file that contains the list of targets, scan results, and scan notes.</td>
<td>n/a</td>
</tr>
<tr>
<td>PDF</td>
<td>An Adobe .pdf file that contains the list of targets, scan results, and scan notes.</td>
<td>n/a</td>
</tr>
</tbody>
</table>

**Note:** Tenable.io cannot export PDF files with more than 400,000 individual scan results.

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Format Description</th>
<th>Exportable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nessus</td>
<td>A .nessus file in XML format that contains the list of targets, scan settings defined by the user, and scan results. Password credentials are stripped so they are not exported as plain text in the XML.</td>
<td>n/a</td>
</tr>
</tbody>
</table>
### CSV
A .csv text file with only scan results. | n/a

### JSON
A .json file that contains the list of targets, scan settings defined by the user, scan results, and scan notes. Password credentials are stripped so they are not exported as plain text in the .json file. | n/a

6. For Vulnerability Management scans, if you select the **PDF - Custom** or **HTML - Custom** formats:
   - Retain the default **Data** setting (**Vulnerabilities** selected).
   - Select either **Assets** or **Plugin** from the **Group By** list, depending on how you want to group the scan results in the export file.

7. Click **Export**.

   Tenable.io generates the export file. Depending on your browser settings, your browser may automatically download the export file to your computer, or may prompt you to confirm the download before continuing.
Scan Templates and Settings

Scan templates contain granular configuration settings for your scans. Tenable.io supports four types of templates:

- Tenable-provided scanner templates
- Tenable-provided agent templates
- Tenable-provided Web Application Scanning templates (requires Tenable.io Web Application Scanning)
- User-defined templates

For more information about scan template types, see Scan Templates.

For more information about template settings, see Scan Settings.
Scan Templates

Scan templates contain granular configuration settings for your scans. The following table describes the scan templates Tenable.io supports.

You can view all available scan templates (Tenable-provided and user-defined) on the templates page when you create a scan.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tenable-provided scanner template</strong></td>
<td>Contains a predefined set of settings recommended for a specific scanning purpose.</td>
</tr>
<tr>
<td><strong>Tenable-provided agent template</strong></td>
<td>Contains a predefined set of settings recommended for a specific agent scanning purpose.</td>
</tr>
<tr>
<td><strong>Tenable-provided Web Application template</strong></td>
<td>Contains a predefined set of settings recommended for a specific web application scanning purpose.</td>
</tr>
<tr>
<td><strong>User-defined template</strong></td>
<td>Contains a custom set of settings that you want to configure for a scan. After you create user-defined templates, you can view and modify them on the Templates page.</td>
</tr>
</tbody>
</table>
# Tenable-Provided Scanner Templates

Tenable provides the following scanner templates for specific scanning purposes. For general information about scan templates and settings, see [Scan Templates and Settings](#).

**Note:** If a plugin requires authentication or settings to communicate with another system, the plugin is not available on agents. This includes, but is not limited to:

- Patch management.
- Mobile device management.
- Cloud infrastructure audit.
- Database checks that require authentication.

Instead, use Tenable-provided [agent templates](#) for agent scanning.

Scanner templates fall into three categories: **Vulnerability Scans (Common)**, **Configuration Scans**, and **Tactical Scans**.

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerability Scans (Common)</strong></td>
<td></td>
</tr>
<tr>
<td>Advanced Network Scan</td>
<td>A scan without any recommendations, so that you can fully customize the scan settings.</td>
</tr>
<tr>
<td>Basic Network Scan</td>
<td>Performs a full system scan that is suitable for any host. For example, you could use this template to perform an internal vulnerability scan on your organization’s systems.</td>
</tr>
<tr>
<td>Credentialed Patch Audit</td>
<td>Authenticates hosts and enumerates missing updates.</td>
</tr>
<tr>
<td>Host Discovery</td>
<td>Performs a simple scan to discover live hosts and open ports.</td>
</tr>
<tr>
<td>Internal PCI Network Scan</td>
<td>Performs an internal PCI DSS (11.2.1) vulnerability scan.</td>
</tr>
<tr>
<td>Legacy Web App Scan</td>
<td>Uses a Nessus scanner to scan your web applications.</td>
</tr>
</tbody>
</table>

**Note:** Unlike the Tenable.io Web Application Scanning scanner, the Nessus scanner does not use a browser to scan your web applications.
<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Device Scan</td>
<td>Assesses mobile devices via Microsoft Exchange or an MDM.</td>
</tr>
<tr>
<td>PCI Quarterly External Scan</td>
<td>Performs quarterly external scans as required by PCI.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Because the nature of a PCI ASV scan is more paranoid and may lead to false positives, the scan data is not included in the aggregate Tenable.io data. This is by design.</td>
</tr>
<tr>
<td><strong>Configuration Scans</strong></td>
<td></td>
</tr>
<tr>
<td>Audit Cloud Infrastructure</td>
<td>Audits the configuration of third-party cloud services.</td>
</tr>
<tr>
<td>MDM Config Audit</td>
<td>Audits the configuration of mobile device managers.</td>
</tr>
<tr>
<td>Offline Config Audit</td>
<td>Audits the configuration of network devices.</td>
</tr>
<tr>
<td>Policy Compliance Auditing</td>
<td>Audits system configurations against a known baseline.</td>
</tr>
<tr>
<td>SCAP and OVAL Auditing</td>
<td>Audits systems using SCAP and OVAL definitions.</td>
</tr>
<tr>
<td><strong>Tactical Scans</strong></td>
<td></td>
</tr>
<tr>
<td>Active Directory Starter Scan</td>
<td>Scans for misconfigurations in Active Directory.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Active Directory Starter Scans require ADSI credentials. For more information, see Miscellaneous.</td>
</tr>
<tr>
<td>Badlock Detection</td>
<td>Performs remote and local checks for CVE-2016-2118 and CVE-2016-0128.</td>
</tr>
<tr>
<td>Bash Shellshock</td>
<td>Performs remote and local checks for CVE-2014-6271 and CVE-2014-</td>
</tr>
<tr>
<td>Template</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Detection</td>
<td>7169.</td>
</tr>
<tr>
<td>DROWN Detection</td>
<td>Performs remote checks for CVE-2016-0800.</td>
</tr>
<tr>
<td>Malware Scan</td>
<td>Scans for malware on Windows and Unix systems.</td>
</tr>
<tr>
<td></td>
<td>Video: Perform a Malware Scan in Tenable.io</td>
</tr>
<tr>
<td></td>
<td>Video: Application, Malware, and Content Audits</td>
</tr>
<tr>
<td>PrintNightmare</td>
<td>Performs local checks for CVE-2021-34527, the PrintNightmare Windows Print Spooler vulnerability.</td>
</tr>
<tr>
<td>Shadow Brokers Scan</td>
<td>Scans for vulnerabilities disclosed in the Shadow Brokers leaks.</td>
</tr>
<tr>
<td>Solorigate</td>
<td>Detects SolarWinds Solorigate vulnerabilities using remote and local checks.</td>
</tr>
<tr>
<td>WannaCry Ransomware Detection</td>
<td>Scans for the WannaCry ransomware.</td>
</tr>
<tr>
<td>Zerologon Remote Scan</td>
<td>Detects Microsoft Netlogon elevation of privilege vulnerability (Zerologon).</td>
</tr>
</tbody>
</table>
Tenable-Provided Agent Templates

You can use templates to create an agent scan configuration or user-defined scan template.

In Tenable.io, Tenable-provided templates for agent scans appear in the **Agent** tab. The interface provides brief explanations of each default template.

**Note:** If you create custom templates for agent scans, those templates appear in the **User Defined** tab.

The table below briefly describes the settings for the default agent scan templates.

For a comprehensive explanation of template settings, see the [Nessus Manager Scan and Policy Settings](#) or [Tenable.io Scan Settings](#).

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Agent Scan</td>
<td>Scans without any recommendations.</td>
</tr>
<tr>
<td><strong>Note:</strong> When you create an agent scan using the Advanced Agent Scan template, you must also select the plugins you want to use for the scan.</td>
<td></td>
</tr>
<tr>
<td>Basic Agent Scan</td>
<td>Scans systems connected via Nessus Agents.</td>
</tr>
<tr>
<td>Custom Agent Scan</td>
<td>Scans using a previously defined template.</td>
</tr>
<tr>
<td>Malware Scan</td>
<td>Scans for malware on systems connected via Nessus Agents.</td>
</tr>
<tr>
<td>Policy Compliance Auditing</td>
<td>Audits systems connected via Nessus Agents.</td>
</tr>
<tr>
<td>SCAP and OVAL Agent Auditing</td>
<td>Audits systems using SCAP and OVAL definitions.</td>
</tr>
</tbody>
</table>
TenableProvided WAS Templates

**Note:** This topic describes scan templates in the new interface only. If you activate the new interface, you can use the classic interface to view a snapshot of historical scan templates you created and configured prior to activating the new interface. However, you can modify scan configurations in the new interface only.

When you activate the new interface, be aware of the following changes:

- In the new interface, the **Legacy Web App Scan** template appears in the **Scanner** tab.
- If you want to create or modify a scan or user-defined scan template based on the **PCI WAS Scan** template, you can use the classic interface only.

For a list of templates and settings available in the classic interface, see WAS Scan Templates (Classic Interface).

Tenable.io Web Application Scanning provides scanner templates for specific scanning purposes. For general information about scan templates and settings, see Scan Templates and Settings.

Tenable.io Web Application Scanning provides the following scanner templates.

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>API</td>
<td>A scan that checks an API for vulnerabilities. This scan analyzes RESTful APIs described via an OpenAPI (Swagger) specification file.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> If the API you want to scan requires keys or a token for authentication, you can add the expected custom headers in the Advanced settings in the HTTP Settings section.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The API scan template is available as a public beta. Its functionality is subject to change as ongoing improvements are made throughout the beta period.</td>
</tr>
<tr>
<td>Config Audit</td>
<td>A high-level scan that analyzes HTTP security headers and other externally-facing configurations on a web application to determine if the application is compliant with common security industry standards.</td>
</tr>
<tr>
<td></td>
<td>If you create a scan using the <strong>Config Audit</strong> scan template, Tenable.io Web Application Scanning analyzes your web application only for plugins related to</td>
</tr>
<tr>
<td>Security Industry Standards Compliance.</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td></td>
</tr>
<tr>
<td>A high-level preliminary scan that determines which URLs in a web application Tenable.io Web Application Scanning scans by default.</td>
<td></td>
</tr>
<tr>
<td>The <strong>Overview</strong> scan template does not analyze the web application for active vulnerabilities. Therefore, this scan template does not offer as many plugin family options as the <strong>Scan</strong> template.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> This scan template is equivalent to the <strong>Web App Overview</strong> template in the classic Tenable.io Web Application Scanning interface.</td>
<td></td>
</tr>
<tr>
<td>PCI</td>
<td></td>
</tr>
<tr>
<td>A scan that assesses web applications for compliance to the Payment Card Industry Data Security Standards (PCI DSS) for PCI ASV.</td>
<td></td>
</tr>
<tr>
<td><strong>Scan</strong></td>
<td></td>
</tr>
<tr>
<td>A comprehensive scan that assesses web applications for a wide range of vulnerabilities.</td>
<td></td>
</tr>
<tr>
<td>The <strong>Scan</strong> template provides plugin family options for all active web application plugins.</td>
<td></td>
</tr>
<tr>
<td>If you create a scan using the <strong>Scan</strong> template, Tenable.io Web Application Scanning analyzes your web application for all plugins that the scanner checks for when you create a scan using the <strong>Config Audit, Overview</strong>, or <strong>SSL TLS</strong> templates, as well as additional plugins to detect specific vulnerabilities.</td>
<td></td>
</tr>
<tr>
<td>A scan run with this scan template provides a more detailed assessment of a web application and take longer to complete that other Tenable.io Web Application Scanning scans.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> This scan template is equivalent to the <strong>Web App Scan</strong> template in the classic Tenable.io Web Application Scanning interface.</td>
<td></td>
</tr>
<tr>
<td>SSL TLS</td>
<td></td>
</tr>
<tr>
<td>A scan to determine if a web application uses SSL/TLS public-key encryption and, if so, how the encryption is configured.</td>
<td></td>
</tr>
<tr>
<td>When you create a scan using the <strong>SSL TLS</strong> template, Tenable.io Web Application Scanning analyzes your web application only for plugins related to SSL/TLS implementation. The scanner does not crawl URLs or assess individual pages for vulnerabilities.</td>
<td></td>
</tr>
</tbody>
</table>
The settings you can configure in a scan or in a user-defined scan template depend on the Tenable-provided scan template type you use to create your scan.
User-Defined Templates

**Note:** Tenable is releasing the new Tenable.io Web Application Scanning interface to users in a rolling fashion. User-defined scan templates are available in the new interface only. This document applies only to organizations where the new interface is enabled.

You can create and configure user-defined policies in the classic interface.

Tenable provides a variety of scan templates for specific scanning purposes. If you want to customize a Tenable-provided scan template and share it with other users, you can create a user-defined scan template.

For information about any scan settings, see [Scan Settings](#).

This section contains information about the following tasks:
Create a User-Defined Template

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Manager or Administrator

You can create user-defined scan templates to save and share custom scan settings with other Tenable.io users. For more information, see [User-Defined Templates](#).

When you define a scan template, Tenable.io assigns you owner permissions for the scan template. You can share the scan template by assigning [template permissions](#) to other users, but only you can [delete](#) the scan template.

To create a user-defined scan template:

1. In the upper-left corner, click the  button.

   The left navigation plane appears.

2. Do one of the following:

   - In the left navigation plane, in the **Vulnerability Management** section, click **Scan Templates**.

     The **Scan Templates** page appears.

   - In the left navigation plane, in the **Web App Scanning** section, click **Scan Templates**.

     The **Scan Templates** page appears.

3. In the upper-right corner of the page, click the  button.

   The **Select a Template** page appears.

4. Click the tile for the template you want to use as the base for your user-defined scan template.

   The **Create a Template** page appears.

5. Configure options for the scan template:
<table>
<thead>
<tr>
<th>Tab</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerability Management Scans</strong></td>
<td><strong>Settings</strong> Configure the settings available in the template.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Basic Settings</strong> – Specifies the organizational and security-related aspects of a scan template. This includes specifying the name of the scan, its targets, whether you want to schedule the scan, and who has permissions for the scan.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Discovery Settings</strong> – Specifies how a scan performs discovery and port scanning.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Assessment Settings</strong> – Specifies how a scan identifies vulnerabilities, as well as what vulnerabilities are identified. This includes identifying malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility of web applications.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Report Settings</strong> – Specifies whether the scan generates a report.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Advanced Settings</strong> – Specifies advanced controls for scan efficiency.</td>
</tr>
<tr>
<td><strong>Credentials</strong></td>
<td>Specify credentials you want Tenable.io to use to perform a credentialed scan.</td>
</tr>
<tr>
<td><strong>Compliance/SCAP</strong></td>
<td>Specify the platforms you want to audit. Tenable provides best practice audits for each platform. Additionally, you can upload a custom audit file.</td>
</tr>
<tr>
<td><strong>Plugins</strong></td>
<td>Select security checks by plugin family or individual plugin.</td>
</tr>
<tr>
<td><strong>Web Application Scans</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Settings</strong></td>
<td>Specifies the organizational and security-related aspects of a scan template. This includes specifying the name of the scan, its targets, whether you want to schedule the scan, and who has permissions for the scan.</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td>Specifies the URLs and file types you want included in or excluded from the scope of your scan.</td>
</tr>
<tr>
<td><strong>Assessment</strong></td>
<td>Specifies how a scan identifies vulnerabilities, as well as what vulnerabilities are identified. This includes identifying malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility of web applications.</td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td>Specifies advanced controls for scan efficiency.</td>
</tr>
<tr>
<td><strong>Credentials</strong></td>
<td>Specify credentials you want Tenable.io to use to perform a credentialed scan.</td>
</tr>
<tr>
<td><strong>Plugins</strong></td>
<td>Select security checks by plugin family or individual plugin.</td>
</tr>
</tbody>
</table>

6. **Click** `Save`.  

Tenable.io saves the user-defined scan template and adds it to the list of scan templates on the Scan Templates page.
Edit a User-Defined Template

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Manager or Administrator

**Required Template Permissions:** Can Configure

To edit a user-defined scan template:

1. In the upper-left corner, click the  button.
   
The left navigation plane appears.

2. Do one of the following:
   
   - In the left navigation plane, in the Vulnerability Management section, click Scan Templates.
   
   The Scan Templates page appears.
   
   - In the left navigation plane, in the Web App Scanning section, click Scan Templates.
   
   The Scan Templates page appears.

3. In the scan templates table, click the scan template you want to edit.
   
The Edit a Scan Template page appears.

4. Configure options for the scan template:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Management Scans</td>
<td>Configure the settings available in the template.</td>
</tr>
<tr>
<td>Settings</td>
<td>Basic Settings – Specifies the organizational and security-related aspects of a scan template. This includes specifying the name of the scan, its targets, whether you</td>
</tr>
</tbody>
</table>
want to schedule the scan, and who has permissions for the scan.

- **Discovery Settings** – Specifies how a scan performs discovery and port scanning.
- **Assessment Settings** – Specifies how a scan identifies vulnerabilities, as well as what vulnerabilities are identified. This includes identifying malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility of web applications.
- **Report Settings** – Specifies whether the scan generates a report.
- **Advanced Settings** – Specifies advanced controls for scan efficiency.

<table>
<thead>
<tr>
<th>Credentials</th>
<th>Specify credentials you want Tenable.io to use to perform a credentialed scan.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance/SCAP</td>
<td>Specify the platforms you want to audit. Tenable provides best practice audits for each platform. Additionally, you can upload a custom audit file.</td>
</tr>
<tr>
<td>Plugins</td>
<td>Select security checks by plugin family or individual plugin.</td>
</tr>
<tr>
<td>Web Application Scans</td>
<td></td>
</tr>
<tr>
<td><strong>Settings</strong></td>
<td>Specifies the organizational and security-related aspects of a scan template. This includes specifying the name of the scan, its targets, whether you want to schedule the scan, and who has permissions for the scan.</td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td>Specifies the URLs and file types you want included in or excluded from the scope of your scan.</td>
</tr>
<tr>
<td><strong>Assessment</strong></td>
<td>Specifies how a scan identifies vulnerabilities, as well as what</td>
</tr>
</tbody>
</table>
vulnerabilities are identified. This includes identifying malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility of web applications.

<table>
<thead>
<tr>
<th>Advanced</th>
<th>Specifies advanced controls for scan efficiency.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credentials</td>
<td>Specify credentials you want Tenable.io to use to perform a credentialed scan.</td>
</tr>
<tr>
<td>Plugins</td>
<td>Select security checks by plugin family or individual plugin.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

Tenable.io saves the user-defined scan template and adds it to the list of templates on the **Scan Templates** page.
Copy a User-Defined Template

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Manager or Administrator

**Required Policy Permissions:** Can Configure

When you copy a user-defined scan template, Tenable.io assigns you owner permissions for the copy. You can share the copy by assigning template permissions to other users, but only you can delete the copied scan template.

To copy a user-defined scan template:

1. In the upper-left corner, click the button.
   
The left navigation plane appears.

2. Do one of the following:
   
   - In the left navigation plane, in the Vulnerability Management section, click Scan Templates.
     
     The Scan Templates page appears.
   
   - In the left navigation plane, in the Web App Scanning section, click Scan Templates.
     
     The Scan Templates page appears.

3. In the scan templates table, roll over the template you want to copy.
   
   The action buttons appear in the row.

4. In the row, click the button.

   A Template successfully copied message appears. Tenable.io creates a copy of the scan template with Copy of prepended to the name and assigns you owner permissions for the copy. The copy appears in the scan templates table.
Export a User-Defined Template

**Required Tenable.io Vulnerability Management User Role:** Standard, Scan Manager, or Administrator

**Required Policy Permissions:** Can Configure

You can export a user-defined scan template for later import.

**Note:** Tenable.io does not export passwords or .audit files in user-defined scan templates.

To export a user-defined scan template:

1. In the upper-left corner, click the ⬅️ button.
   
The left navigation plane appears.

2. In the left navigation plane, in the **Vulnerability Management** section, click **Scan Templates**.
   
The **Scan Templates** page appears.

3. In the scan templates table, roll over the scan template you want to export.
   
The action buttons appear in the row.

4. In the row, click the ⬅️ button.
   
   Tenable.io exports the user-defined scan template as a .nessus file.
Import a User-Defined Template

**Required Tenable.io Vulnerability Management User Role:** Standard, Scan Manager, or Administrator

When you import a scan template, Tenable.io assigns you owner permissions for the scan template. You can share the scan template by assigning template permissions to other users, but only you can delete the scan template.

Tenable.io does not include passwords or compliance audit files in exported user-defined scan templates. You must add these settings in manually after importing the scan template.

To import a user-defined scan template:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, in the **Vulnerability Management** section, click **Scan Templates**.
   
   The **Scan Templates** page appears.

3. In the upper-right corner of the page, click the button.
   
   Your file manager appears.

4. Select the scan template you want to import.

5. Click **Open**.
   
   A **Template uploaded successfully** message appears, and the scan template appears on the **Scan Templates** page.

What to do next:

- As needed, add **passwords** and **compliance audit files** to the imported template.
Change User-Defined Template Ownership

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Manager or Administrator

**Required Template Permissions:** Owner

To change the ownership of a user-defined scan template in the new interface:

1. Edit a [Vulnerability Management](#) or [web application](#) scan configuration.

2. In the left navigation menu, in the **Settings** section, click **Basic**.

   The **Basic** settings appear.

3. In the **User Permissions** section, next to the permission drop-down for **Owner**, click the **▼** button.

   A list of available user accounts appears.

4. Select a user from the list.

   Tenable.io automatically adds you to the list of users and assigns **Can Use** permissions to your user account.

5. (Optional) Remove all permissions for your user account:

   - In the user list, roll over your user account.
     
     The **X** button appears at the end of the listing.

   - Click the **X** button.

     Tenable.io removes your account from the list of users.

6. (Optional) Edit **permissions** for your user account:

   - Next to the permission drop-down for your user account, click the **▼** button.

   - Select a permission.

7. Click **Save**.
Tenable assigns ownership to the selected user and assigns your user account the permissions you selected. If you removed all permissions for your user account from the template, the template no longer appears in the templates table.
Delete a User-Defined Template

**Required Tenable.io Vulnerability Management User Role:** Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Manager or Administrator

**Required Template Permissions:** Owner

If you delete a user-defined scan template, Tenable.io deletes it from all user accounts.

Before you begin:

- **Delete** any scans that use the template you want to delete. You cannot delete a scan template if a scan is using the template.

To delete a user-defined scan template or templates:

1. In the upper-left corner, click the **button.

   The left navigation plane appears.

2. Do one of the following:

   - In the left navigation plane, in the **Vulnerability Management** section, click **Scan Templates**.
     
     The **Scan Templates** page appears.

   - In the left navigation plane, in the **Web App Scanning** section, click **Scan Templates**.
     
     The **Scan Templates** page appears.

3. Select the scan template or templates you want to delete:

   - **Select a single scan template**:
     
     a. In the scan templates table, roll over the scan template you want to delete.
       
       The action buttons appear in the row.

     b. In the row, click the **button.
A confirmation window appears.

- **Select multiple scan templates:**
  a. In the scan templates table, select the check box for each scan template you want to delete.
  
  The action bar appears at the bottom of the page.
  b. In the action bar, click the button.

  A confirmation window appears.

4. In the confirmation window, click **Delete**.

Tenable.io deletes the user-defined scan template or templates you selected.
Scan Settings

Scan settings enable you to refine parameters in scans to meet your specific network security needs. The scan settings you can configure vary depending on the Tenable-provided template on which a scan or user-defined template is based.

You can configure these settings in individual scans or in user-defined templates from which you create individual scans.

Scan settings are organized into the following categories:

<table>
<thead>
<tr>
<th>Vulnerability Management Scans</th>
<th>Web Application Scans</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Basic Settings in User-Defined Templates</td>
<td>• Basic Settings in User-Defined Templates</td>
</tr>
<tr>
<td>• Basic Settings in Vulnerability Management Scans</td>
<td>• Basic Settings in WAS Scans</td>
</tr>
<tr>
<td>• Discovery Settings in Vulnerability Management Scans</td>
<td>• Scope Settings in WAS Scans</td>
</tr>
<tr>
<td>• Assessment Settings in Vulnerability Management Scans</td>
<td>• Report Settings in WAS Scans</td>
</tr>
<tr>
<td>• Report Settings in Vulnerability Management Scans</td>
<td>• Assessment Settings in WAS Scans</td>
</tr>
<tr>
<td>• Advanced Settings in Vulnerability Management Scans</td>
<td>• Advanced Settings in WAS Scans</td>
</tr>
<tr>
<td>• Credentials in Vulnerability Management Scans</td>
<td>• Credentials in WAS Scans</td>
</tr>
<tr>
<td>• Compliance in Vulnerability Management Scans</td>
<td>• Plugin Settings in WAS Scans</td>
</tr>
<tr>
<td>• SCAP Settings in Vulnerability Management Scans</td>
<td></td>
</tr>
<tr>
<td>• Configure Plugins in Vulnerability Management Scans</td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective
Settings in User-Defined Templates

When configuring settings for user-defined templates, note the following:

- If you configure a setting in a user-defined template, that setting applies to any scans you create based on that user-defined template.

- You base a user-defined template on a Tenable-provided template. Most of the settings are identical to the settings you can configure in an individual scan that uses the same Tenable-provided template.

However, certain **Basic** settings are unique to creating a user-defined template, and do not appear when configuring an individual scan. For more information, see [Basic Settings in User-Defined Templates](#).

- You can configure certain settings in a user-defined template, but cannot modify those settings in an individual scan based on a user-defined template. These settings include **Discovery**, **Assessment**, **Report**, **Advanced**, **Compliance**, **SCAP**, and **Plugins**. If you want to modify these settings for individual scans, create individual scans based on a Tenable-provided template instead.

- If you configure **Credentials** in a user-defined template, other users can override these settings by adding scan-specific or managed credentials to scans based on the template.
Basic Settings in Vulnerability Management Scans

**Note:** This topic describes **Basic** settings you can set in individual scans. For **Basic** settings in user-defined templates, see [Basic Settings in User-Defined Templates](#).

You can use **Basic** settings to specify organizational and security-related aspects of a scan configuration. This includes specifying the name of the scan, its targets, whether the scan is scheduled, and who has access to the scan.

The **Basic** settings include the following sections:

- **General**
- **Schedule**
- **Notifications**
- **User Permissions**

**General**

The general settings for a scan.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>None</td>
<td>Specifies the name of the scan.</td>
</tr>
<tr>
<td>Description</td>
<td>None</td>
<td>(Optional) Specifies a description of the scan.</td>
</tr>
<tr>
<td>Scan Results</td>
<td>Show in dash-</td>
<td>Specifies whether the results of the scan should appear in dashboards or be</td>
</tr>
<tr>
<td>(board)</td>
<td></td>
<td>kept private.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When set to <strong>Keep private</strong>, you must access the scan directly to view the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>results.</td>
</tr>
<tr>
<td>Folder</td>
<td>My Scans</td>
<td>Specifies the folder where the scan appears after being saved.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You cannot specify a folder when you launch a remediation scan. All remedia-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tion scans appear in the <strong>Remediation Scans</strong> folder only.</td>
</tr>
<tr>
<td><strong>Agent Groups</strong></td>
<td>None</td>
<td>(Agent scans only) Specifies the <a href="#">agent group</a> or groups you want the scan to target. In the drop-down box, select an existing agent group, or create a new agent group.</td>
</tr>
<tr>
<td>------------------</td>
<td>------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Scan Window</strong></td>
<td>1 hour</td>
<td>(Agent scans only) <em>(Required)</em> Specifies the time frame during which agents must report in order to be included and visible in vulnerability reports. Use the drop-down box to select an interval of time, or click <img src="#" alt="click" /> to type a custom scan window.</td>
</tr>
</tbody>
</table>
| **Scanner**      | Auto-Select | Specifies the scanner that performs the scan. Select a scanner based on the location of the targets you want to scan. For example:  
  - Select a [linked scanner](#) to scan non-routable IP addresses.  
  
  **Note:** Auto-select is not available for [cloud scanners](#).  
  - Select a [scanner group](#) if you want to:  
    - Improve scan speed by balancing the scan load among multiple scanners.  
    - Rebuild scanners and link new scanners in the future without having to update scanner designations in scan configurations.  
  - Select [Auto-Select](#) to enable [scan routing](#) for the targets. |
| **IP Selection** | Internal | *(Required)* Select whether to run an [Internal](#) or [External](#) tag-based scan. Tenable.io evaluates the identifiers to determine a single target in the following order:  
  **External:** Public routable IP addresses. Tenable.io evaluates the identifiers to determine a single target in the following order: |
<table>
<thead>
<tr>
<th>Internal: Privately routable IP addresses (RFC 1918). Tenable.io evaluates the identifiers in the same order as External.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> This option determines the type of scan run of assets within the tag(s). For example, if you are using a cloud scanner but want to scan the public targets in the tag, you must change the IP selection to <strong>External</strong>.</td>
</tr>
<tr>
<td>Scan routing is available for linked scanners only.</td>
</tr>
</tbody>
</table>

| Tags | None | Select one or more **tags** to scan all assets that have any of the specified tags applied. To see a list of assets identified by the specified tags, click **View Assets**. For more information, see [Example: Tag-Based Scanning](#). |
|---|
| **Target Groups** | None | You can select or add a new target group to which the scan applies. Assets in the target group are used as scan targets. |
| **Policy** | None | This setting appears only when the scan owner edits an existing scan that is based on a **user-defined scan template**. |
| **Note:** After scan creation, you cannot change the Tenable-provided scan template on which a scan is based. |
| In the drop-down box, select a user-defined scan template on which to base the scan. You can select user-defined scan templates for which you have **Can View** or higher permissions. |
In most cases, you set the user-defined scan template at scan creation, then keep the same template each time you run the scan. However, you may want to change the user-defined scan template when troubleshooting or debugging a scan. For example, changing the template makes it easy to enable or disable different plugin families, change performance settings, or apply dedicated debugging templates with more verbose logging.

When you change the user-defined scan template for a scan, the scan history retains the results of scans run under the previously-assigned template.

<table>
<thead>
<tr>
<th>Targets</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies one or more targets to be scanned. If you select a target group or upload a targets file, you are not required to specify additional targets.</td>
<td></td>
</tr>
<tr>
<td>Targets can be specified using a number of different formats.</td>
<td></td>
</tr>
<tr>
<td>The targets you specify must be appropriate to the scanner you select for the scan. For example, cloud scanners cannot scan non-routable IP addresses. Select an internal scanner instead.</td>
<td></td>
</tr>
</tbody>
</table>

**Tip:** You can force Tenable.io to use a given host name for a server during a scan by using the `hostname[ip]` syntax (e.g., `www.example.com[192.168.1.1]`). However, you cannot use this approach if you enable scan routing for the scan.

**Note:** You cannot apply more than 300,000 IP address targets to a scan.

<table>
<thead>
<tr>
<th>Upload Targets</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uploads a text file that specifies targets.</td>
<td></td>
</tr>
<tr>
<td>The targets file must be formatted in the following manner:</td>
<td></td>
</tr>
<tr>
<td>- ASCII file format</td>
<td></td>
</tr>
</tbody>
</table>
Schedule

The scan schedule settings.

By default, scans are not scheduled. When you first access the Schedule section, the Enable Schedule setting appears, set to Off. To modify the settings listed on the following table, click the Off button. The rest of the settings appear.

**Note:** Scheduled scans do not run if they are in the scan owner’s Trash folder.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>Once</td>
<td>Specifies how often the scan is launched.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Once:</strong> Schedule the scan at a specific time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Daily:</strong> Schedule the scan to occur every 1-20 days, at a specific time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Weekly:</strong> Schedule the scan to occur every 1-20 weeks, by time and day(s) of the week.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Monthly:</strong> Schedule the scan to occur every 1-20 months, by time and day or week of the month.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> If you schedule your scan to recur monthly, Tenable recommends setting a start date no later than the 28th day. If you select a start date that does not exist in some months (e.g., the 29th), Tenable.io cannot run the scan on those days.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Yearly:</strong> Schedule the scan to occur every 1-20 years, by</td>
</tr>
</tbody>
</table>

Note: Unicode/UTF-8 encoding is not supported.
Starts | Varies | Specifies the exact date and time when a scan launches. The starting date defaults to the date when you are creating the scan. The starting time is the nearest half-hour interval. For example, if you create your scan on 09/31/2018 at 9:12 AM, the default starting date and time is set to 09/31/2018 and 09:30.

Timezone | Zulu | Specifies the timezone of the value set for Starts.

Repeat Every | Varies | Specifies the interval at which a scan is relaunched. The default value of this item varies based on the frequency you choose.

Repeat On | Varies | Specifies what day of the week a scan repeats. This item appears only if you specify Weekly for Frequency. The value for Repeat On defaults to the day of the week on which you create the scan.

Repeat By | Day of the Month | Specifies when a monthly scan is relaunched. This item appears only if you specify Monthly for Frequency.

Summary | N/A | Provides a summary of the schedule for your scan based on the values you have specified for the available settings.

Notifications

The notification settings for a scan.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Recipient(s)</td>
<td>None</td>
<td>Specifies zero or more email addresses, separated by commas, that are alerted when a scan completes and the results are available.</td>
</tr>
<tr>
<td>Result Filters</td>
<td>None</td>
<td>Defines the type of information to be emailed.</td>
</tr>
</tbody>
</table>
User Permissions

You can share the scan with other users by setting permissions for users or groups. When you assign a permission to a group, that permission applies to all users within the group.

**Tip:** Tenable recommends assigning permissions to user groups, rather than individual users, to minimize maintenance as individual users leave or join your organization.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Access</td>
<td>(Default user only) Groups and users set to this permission cannot interact with the scan in any way.</td>
</tr>
<tr>
<td>Can View</td>
<td>Groups and users with this permission can view the results of the scan, export the scan results, and move the scan to the Trash folder. They cannot view the scan configuration or permanently delete the scan.</td>
</tr>
<tr>
<td>Can Control</td>
<td>In addition to the tasks allowed by Can View, groups and users with this permission can launch, pause, and stop a scan. They cannot view the scan configuration or permanently delete the scan.</td>
</tr>
<tr>
<td>Can Configure</td>
<td>In addition to the tasks allowed by Can Control, groups and users with this permission can view the scan configuration and modify any setting for the scan except scan ownership. They can also delete the scan.</td>
</tr>
</tbody>
</table>

**Note:** In addition to Can Control permissions for the scan, users running a scan must have Can Scan permissions in an access group for the specified target, or the scanner does not scan the target.

**Note:** Only the scan owner can change scan ownership.

**Note:** User roles override scan permissions in the following cases:

- A basic user cannot run a scan or configure a scan, regardless of the permissions assigned to that user in the individual scan.
- An administrator always has the equivalent of Can Configure permissions, regardless of the permissions set for the administrator account in the individual scan.
Scan Targets

In Tenable.io, you can use a number of different formats when specifying targets for a scan. The following tables contain target formats, examples, and a short explanation of what occurs when Tenable.io scans that target type.

**Note:** For previously scanned assets, you can configure scan targets based on host attributes like operating system or installed software, instead of host identifiers like IP address. For more information, see Example: Tag-Based Scanning.

**Note:** AWS Pre-authorized scanners do not scan the T3.nano, T2.nano, T1.micro, or M1.small targets. For more information, see the AWS Penetration Testing documentation. Additionally, for more information about Pre-Authorized scan targets in Tenable.io, see Basic Settings.

**Tip:** If a hostname target looks like either a link6 target (start with the text "link6") or one of the two IPv6 range forms, put single quotes around the target to ensure that Tenable.io processes it as a hostname.

<table>
<thead>
<tr>
<th>Target Description</th>
<th>Example</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>A single IPv4 address</td>
<td>192.168.0.1</td>
<td>Scans the single IPv4 address.</td>
</tr>
<tr>
<td>A single IPv6 address</td>
<td>2001:db8::2120:17ff:fe56:333b</td>
<td>Scans the single IPv6 address.</td>
</tr>
<tr>
<td>A single link local IPv6 address with a scope identifier</td>
<td>fe80:0:0:0:216:cbff:fe92:88d0%eth0</td>
<td>Scans the single IPv6 address. Note that you must use interface indexes, not interface names, for the scope identifier on Windows platforms.</td>
</tr>
<tr>
<td>An IPv4 range with a start and end address</td>
<td>192.168.0.1-192.168.0.255</td>
<td>Scans all IPv4 addresses between the start address and end address, including both addresses.</td>
</tr>
<tr>
<td>An IPv4 address with</td>
<td>192.168.0-1.3-5</td>
<td>Scans all combinations of the values given in the octet.</td>
</tr>
<tr>
<td>Target Description</td>
<td>Example</td>
<td>Explanation</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>one or more octets replaced with numeric ranges</td>
<td></td>
<td>ranges. In this example, scans: 192.168.0.3, 192.168.0.4, 192.168.0.5, 192.0.2.3, 192.0.2.4 and 192.0.2.5.</td>
</tr>
<tr>
<td>An IPv4 subnet with CIDR notation</td>
<td>192.168.0.0/24</td>
<td>Scans all addresses within the specified subnet. The address given is not the start address. Specifying any address within the subnet with the same CIDR scans the same set of hosts.</td>
</tr>
<tr>
<td>An IPv4 subnet with netmask notation</td>
<td>192.168.0.0/255.255.255.128</td>
<td>Scans all addresses within the specified subnet. The address is not a start address. Specifying any address within the subnet with the same netmask scans the same hosts.</td>
</tr>
<tr>
<td>A host resolvable to either an IPv4 or an IPv6 address</td>
<td><a href="http://www.yourdomain.com">www.yourdomain.com</a></td>
<td>Scans the single host. If Tenable.io can resolve the hostname to multiple addresses, Tenable.io scans the first resolved IPv4 address or, if Tenable.io cannot resolve an IPv4 address, the first resolved IPv6 address.</td>
</tr>
<tr>
<td>A host resolvable to an IPv4 address with CIDR notation</td>
<td><a href="http://www.yourdomain.com/24">www.yourdomain.com/24</a></td>
<td>Resolves the hostname to an IPv4 address, then scans all addresses within the specified subnet.</td>
</tr>
<tr>
<td>Target Description</td>
<td>Example</td>
<td>Explanation</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>A host resolvable to an IPv4 address with netmask notation</td>
<td><a href="http://www.yourdomain.com/255.255.252.0">www.yourdomain.com/255.255.252.0</a></td>
<td>Tenable.io treats this format like any other IPv4 address with CIDR notation. Resolves the hostname to an IPv4 address, then scans all addresses within the specified subnet. Tenable.io treats this format like any other IPv4 address with netmask notation.</td>
</tr>
<tr>
<td>The text 'link6' optionally followed by an IPv6 scope identifier</td>
<td>link6 or link6%16</td>
<td>Scans all hosts that respond to multicast ICMPv6 echo requests sent out on the interface specified by the scope identifier to the ff02::1 address. If no IPv6 scope identifier is given, the requests are sent out on all interfaces. Note that you must use interface indexes, not interface names, for the scope identifier on Windows platforms.</td>
</tr>
<tr>
<td>Some text with either a single IPv4 or IPv6 address within square brackets</td>
<td>&quot;Test Host 1[10.0.1.1]&quot; or &quot;Test Host 2 [2001:db8::abcd]&quot;</td>
<td>Scans the IPv4 or IPv6 address within the brackets, like a normal single target.</td>
</tr>
</tbody>
</table>
Basic Settings in WAS Scans

Configure **settings** to specify basic organizational and security-related aspects of your scan configuration. This includes specifying the name of the scan, its target, whether the scan is scheduled, and who has access to the scan.

You can configure **settings** when you create a scan or user-defined scan template and select any scan type. For more information, see [Scan Templates](#).

**Tip:** If you want to save your settings configurations and apply them to other scans, you can create and configure a user-defined scan template.

The **Basic** settings include the following sections:

- **General**
- **Schedule**
- **Notifications**
- **User Permissions**
- **Data Sharing**

### General

The general settings for a scan.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>none</td>
<td>Specifies the name of the scan or template.</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>none</td>
<td>Specifies a description of the scan or template.</td>
<td>No</td>
</tr>
<tr>
<td>Target</td>
<td>none</td>
<td>Specifies the URL for the target you want to scan, as it appears on your Tenable.io Web Application Scanning license. Regular expressions and wildcards are not allowed.</td>
<td>Yes</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>---------</td>
<td>---------------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>Folder</td>
<td>My Scans</td>
<td>Specifies the folder where the scan appears after being saved.</td>
<td>Yes</td>
</tr>
<tr>
<td>Scanner</td>
<td>varies</td>
<td>Specifies the scanner that performs the scan.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Note:** If the URL you type in the Target box has a different FQDN host from the URL that appears on your license, and your scan runs successfully, the new URL you type counts as an additional asset on your license.

**Note:** If you create a user-defined scan template, the target setting is not saved to the template. You must type a target each time you create a new scan.

### Schedule

The schedule settings for the scan.

**Note:** If you create a user-defined scan template, your schedule settings are not saved to the scan template. You must configure the schedule settings each time you create a new scan.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule</td>
<td>off</td>
<td>A toggle that specifies whether the scan is scheduled. By default, scans are not scheduled. When the Schedule toggle is disabled, the other schedule settings remain hidden. Click the toggle to enable the schedule and view the remaining Schedule settings.</td>
</tr>
<tr>
<td>Frequency</td>
<td>Once</td>
<td>Specifies how often the scan is launched.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong>: The frequency with which you scan your target depends on several factors (e.g., how often you update your web application, the content your web application contains, etc.). For most web applications, Tenable recommends at least monthly scans.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Once</strong>: Schedule the scan at a specific time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Daily</strong>: Schedule the scan to occur on a daily basis, at a specific time, up to 20 days.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Weekly</strong>: Schedule the scan to occur on a recurring basis, by time and day of week, up to 20 weeks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Monthly</strong>: Schedule the scan to occur every month, by time and day of month or week of month, up to 20 months.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Yearly</strong>: Schedule the scan to occur every year, by time and day, up to 20 years.</td>
</tr>
<tr>
<td>Starts</td>
<td>varies</td>
<td>Specifies the exact date and time at which a scan launches.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong>: If you schedule an excessive number of scans to run concurrently, you may exhaust the scanning capacity on Tenable.io Web Application Scanning. If necessary, Tenable.io Web Application Scanning staggers concurrent scans to ensure consistent scanning performance.</td>
</tr>
<tr>
<td>Timezone</td>
<td>varies</td>
<td>The starting date defaults to the date you create the scan. The starting time is the next hour interval, displayed in 24-hour clock format. For example, if you create your scan on October 31, 2019 at 9:12 PM, the default starting date and time is 10/31/2019 and 22:00.</td>
</tr>
</tbody>
</table>

**Notifications**

The notification settings for a scan.
### User Permissions

Share the scan or user-defined scan template with other users by setting permissions for users. For more information on adding or editing user permissions, see [Set WAS Scan Permissions](#).

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Access</td>
<td>(Default) Users set to this permission cannot interact with the scan in any way.</td>
</tr>
<tr>
<td>Can View</td>
<td>Users set to this permission can view the results of the scan.</td>
</tr>
<tr>
<td>Can Control</td>
<td>In addition to the tasks allowed by Can View, users with this permission can launch and stop a scan. They cannot view or edit the scan configuration or delete the scan.</td>
</tr>
<tr>
<td>Can Configure</td>
<td>In addition to the tasks allowed by Can Control, users with this permission can view the scan configuration and modify any setting for the scan except scan ownership. They can also delete the scan.</td>
</tr>
</tbody>
</table>

---

### Data Sharing

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Results</td>
<td>Show in dashboard</td>
<td>Specifies whether the results of the scan should be kept private or should appear on users' dashboards. When set to <strong>Keep private</strong>, users must access the scan directly to view the results.</td>
</tr>
</tbody>
</table>
Basic Settings in User-Defined Templates

Note: This topic describes Basic settings you can set in user-defined templates. For Basic settings in individual scans, see Basic Settings in Vulnerability Management Scans.

You can use Basic settings to specify basic aspects of a user-defined template, including who has access to the user-defined template.

The Basic settings include the following sections:

- **General**
- **Permissions**

General

The general settings for a user-defined template.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>None</td>
<td>Specifies the name of the user-defined template.</td>
</tr>
<tr>
<td>Description</td>
<td>None</td>
<td>(Optional) Specifies a description of the user-defined template.</td>
</tr>
</tbody>
</table>

Permissions

You can share the user-defined template with other users by setting permissions for users or groups. When you assign a permission to a group, that permission applies to all users within the group.

Tip: Tenable recommends assigning permissions to user groups, rather than individual users, to minimize maintenance as individual users leave or join your organization.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Access</td>
<td>(Default user only) Groups and users set to this permission cannot interact with the user-defined template in any way.</td>
</tr>
</tbody>
</table>
Can Use Groups and users with this permission can view the template configuration and use the template to create scans.

Can Edit In addition to viewing the template and using the template to create scans, groups and users with this permission can modify any template settings except user permissions and template ownership. However, they cannot export or delete the template.

Can Configure In addition to viewing the template and using the template to create scans, groups and users with this permission can modify any setting for the template except template ownership. They can export the template, but cannot delete the template.

**Note:** Only the template owner can delete a template.

## Authentication

In user-defined templates, you can use **Authentication** settings to configure the authentication Tenable.io performs for credentialed scanning.

**Tip:** The Authentication settings are equivalent to the Scan-wide Credential Type Settings in Tenable-provided scan templates.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv1/v2c</td>
<td></td>
<td>equivalent to Scans &gt; Credentials &gt; <strong>Plaintext Authentication</strong> &gt; SNMPv1/v2c</td>
</tr>
<tr>
<td>UDP Port</td>
<td>161</td>
<td>Ports where Tenable.io attempts to authenticate on the host device.</td>
</tr>
<tr>
<td>Additional UDP port #1</td>
<td>161</td>
<td></td>
</tr>
<tr>
<td>Additional UDP port #2</td>
<td>161</td>
<td></td>
</tr>
<tr>
<td>Additional UDP port #3</td>
<td>161</td>
<td></td>
</tr>
</tbody>
</table>
### HTTP

*equivalent to Scans > Credentials > Plaintext Authentication > HTTP*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login method</td>
<td>POST</td>
<td>Specify if the login action is performed via a GET or POST request.</td>
</tr>
<tr>
<td>Re-authenticate delay (seconds)</td>
<td>0</td>
<td>The time delay between authentication attempts. Setting a time delay is useful to avoid triggering brute force lockout mechanisms.</td>
</tr>
<tr>
<td>Follow 30x redirects (# of levels)</td>
<td>0</td>
<td>If a 30x redirect code is received from a web server, this setting directs Tenable.io to follow the link provided or not.</td>
</tr>
<tr>
<td>Invert authenticated regex</td>
<td>Disabled</td>
<td>A regex pattern to look for on the login page, that if found, tells Tenable.io that authentication was not successful (e.g., Authentication failed!).</td>
</tr>
<tr>
<td>Use authenticated regex on HTTP headers</td>
<td>Disabled</td>
<td>Rather than search the body of a response, Tenable.io can search the HTTP response headers for a given regex pattern to better determine authentication state.</td>
</tr>
<tr>
<td>Case insensitive authenticated regex</td>
<td>Disabled</td>
<td>The regex searches are case sensitive by default. This instructs Tenable.io to ignore case.</td>
</tr>
</tbody>
</table>

### telnet/rsh/rexec

*equivalent to Scans > Credentials > Plaintext Authentication > telnet/ssh/rexec*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform patch audits over telnet</td>
<td>Disabled</td>
<td>Tenable.io uses telnet to connect to the host device for patch audits.</td>
</tr>
<tr>
<td>Perform patch audits over rsh</td>
<td>Disabled</td>
<td>Tenable.io uses rsh to connect to the host device for patch audits.</td>
</tr>
<tr>
<td>Perform patch audits over rexec</td>
<td>Disabled</td>
<td>Tenable.io uses rexec to connect to the host device for patch audits.</td>
</tr>
</tbody>
</table>
### Windows

*equivalent to Scans > Credentials > **Host** > Windows*

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never send credentials in the clear</td>
<td>Enabled</td>
<td>By default, for security reasons, this option is enabled.</td>
</tr>
<tr>
<td>Do not use NTLMv1 authentication</td>
<td>Enabled</td>
<td>If the <strong>Do not use NTLMv1 authentication</strong> option is disabled, then it is theoretically possible to trick Tenable.io into attempting to log into a Windows server with domain credentials via the NTLM version 1 protocol. This provides the remote attacker with the ability to use a hash obtained from Tenable.io. This hash can be potentially cracked to reveal a username or password. It may also be used to directly log into other servers. Force Tenable.io to use NTLMv2 by enabling the <strong>Only use NTLMv2</strong> setting at scan time. This prevents a hostile Windows server from using NTLM and receiving a hash. Because NTLMv1 is an insecure protocol, this option is enabled by default.</td>
</tr>
<tr>
<td>Start the Remote Registry service during the scan</td>
<td>Disabled</td>
<td>This option tells Tenable.io to start the Remote Registry service on computers being scanned if it is not running. This service must be running in order for Tenable.io to execute some Windows local check plugins.</td>
</tr>
<tr>
<td>Enable administrative shares during the scan</td>
<td>Disabled</td>
<td>This option allows Tenable.io to access certain registry entries that can be read with administrator privileges.</td>
</tr>
</tbody>
</table>

**Note:** This option is disabled by default to improve default scan performance. Additionally, enabling this option can have implications depending on your network security implementation. For example, certain access control configurations for your network firewall might blacklist your scanner for attempting to negotiate Server Message Block Protocol (SMB protocol) connections.
**Note:** This option is disabled by default to improve default scan performance. Additionally, enabling this option can have implications depending on your network security implementation. For example, certain access control configurations for your network firewall might blacklist your scanner for attempting to negotiate Server Message Block Protocol (SMB protocol) connections.

### SSH

**equivalent to Scans > Credentials > Host > SSH**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>known_hosts file</td>
<td>None</td>
<td>If you upload an SSH known_hosts file, Tenable.io only attempts to log in to hosts in this file. This can ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a log into a system that may not be under your control.</td>
</tr>
<tr>
<td>Preferred port</td>
<td>22</td>
<td>The port on which SSH is running on the target system.</td>
</tr>
<tr>
<td>Client version</td>
<td>OpenSSH_5.0</td>
<td>The type of SSH client Tenable.io impersonates while scanning.</td>
</tr>
<tr>
<td>Attempt least privilege</td>
<td>Cleared</td>
<td>Enables or disables dynamic privilege escalation. When enabled, Tenable.io attempts to run the scan with an account with lesser privileges, even if the Elevate privileges with option is enabled. If a command fails, Tenable.io escalates privileges. Plugins 101975 and 101976 report which plugins ran with or without escalated privileges.</td>
</tr>
</tbody>
</table>

**Note:** Enabling this option may increase scan run time by up to 30%.

### Amazon AWS

**equivalent to Scans > Credentials > Cloud Services > Amazon AWS**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regions to access</td>
<td>Rest of the World</td>
<td>In order for Tenable.io to audit an Amazon AWS account, you must define the regions you want to scan.</td>
</tr>
</tbody>
</table>
Per Amazon policy, you need different credentials to audit account configuration for the China region than you do for the rest of the world.

Possible regions include:

- **GovCloud** – If you select this region, you automatically select the government cloud (e.g., us-gov-west-1).

- **Rest of the World** – If you select this region, the following additional options appear:
  - us-east-1
  - us-east-2
  - us-west-1
  - us-west-2
  - ca-central-1
  - eu-west-1
  - eu-west-2
  - eu-central-1
  - ap-northeast-1
  - ap-northeast-2
  - ap-southeast-1
  - ap-southeast-2
  - sa-east-1

- **China** – If you select this region, the following additional options appear:
  - cn-north-1
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>cn-northwest-1</strong></td>
</tr>
<tr>
<td>HTTPS</td>
<td>Enabled</td>
<td>Whether Tenable.io authenticates over an encrypted (HTTPS) or an unencrypted (HTTP) connection.</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>Enabled</td>
<td>Whether Tenable.io verifies the validity of the SSL digital certificate.</td>
</tr>
</tbody>
</table>

## Rackspace

*equivalent to Scans > Credentials > [Cloud Services](#) > Rackspace*

<table>
<thead>
<tr>
<th>Location</th>
<th>-</th>
<th>Location of the Rackspace Cloud instance. Possible locations include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Dallas-Fort Worth (DFW)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Chicago (ORD)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Northern Virginia (IAD)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• London (LON)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sydney (SYD)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Hong Kong (HKG)</td>
</tr>
</tbody>
</table>

## Microsoft Azure

*equivalent to Scans > Credentials > [Cloud Services](#) > Amazon AWS*

| Subscription IDs | -  | List subscription IDs to scan, separated by a comma. If this field is blank, all subscriptions are audited.                          |

## Apple Profile Manager

*equivalent to Scans > Credentials > [Mobile](#) > Apple Profile Manager*

<table>
<thead>
<tr>
<th>Force device updates</th>
<th>Enabled</th>
<th>Force devices to update with Apple Profile Manager immediately.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device update timeout (minutes)</td>
<td>5</td>
<td>Number of minutes to wait for devices to reconnect with Apple Profile Manager.</td>
</tr>
</tbody>
</table>
Discovery Settings in Vulnerability Management Scans

**Note:** If a scan is based on a user-defined template, you cannot configure **Discovery** settings in the scan. You can only modify these settings in the related user-defined template.

The **Discovery** settings relate to discovery and port scanning, including port ranges and methods.

Certain Tenable-provided scanner templates include **preconfigured discovery settings**.

If you select the **Custom** preconfigured setting option, or if you are using a scanner template that does not include preconfigured discovery settings, you can manually configure **Discovery** settings in the following categories:

- **Host Discovery**
- **Port Scanning**
- **Service Discovery**

**Host Discovery**

By default, some settings in the **Host Discovery** section are enabled. When you first access the **Host Discovery** section, the **Ping the remote host** option appears and is set to **On**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping the Remote Host</td>
<td>On</td>
<td>If set to <strong>On</strong>, the scanner pings remote hosts on multiple ports to determine if they are alive. Additional options <strong>General Settings</strong> and <strong>Ping Methods</strong> appear. If set to <strong>Off</strong>, the scanner does not ping remote hosts on multiple ports during the scan. <strong>Note:</strong> To scan VMware guest systems, <strong>Ping the remote host</strong> must be set to <strong>Off</strong>.</td>
</tr>
<tr>
<td>Scan Unresponsive Hosts</td>
<td>Disabled</td>
<td>Specifies whether the Nessus scanner scans hosts that do not respond to any ping methods. This option is only available for scans using the <strong>PCI Quarterly External</strong></td>
</tr>
</tbody>
</table>
### General Settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Fast Network Discovery</td>
<td>Disabled</td>
<td>When disabled, if a host responds to ping, Tenable.io attempts to avoid false positives, performing additional tests to verify the response did not come from a proxy or load balancer. These checks can take some time, especially if the remote host is firewalled. When enabled, Tenable.io does not perform these checks.</td>
</tr>
</tbody>
</table>

### Ping Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>Enabled</td>
<td>Ping a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.</td>
</tr>
<tr>
<td>TCP</td>
<td>Enabled</td>
<td>Ping a host using TCP.</td>
</tr>
<tr>
<td>Destination Ports (TCP)</td>
<td>Built-In</td>
<td>Destination ports can be configured to use specific ports for TCP ping. This specifies the list of ports that are checked via TCP ping. Type one of the following: built-in, a single port, or a comma-separated list of ports. For more information about which ports built-in specifies, see the knowledge base article.</td>
</tr>
<tr>
<td>ICMP</td>
<td>Enabled</td>
<td>Ping a host using the Internet Control Message Protocol (ICMP).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assume ICMP Unreachable From the Gateway Means the Host is Down</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Disabled</td>
<td>Assume ICMP unreachable from the gateway means the host is down. When a ping is sent to a host that is down, its gateway may return an ICMP unreachable message. When this option is enabled, when the scanner receives an ICMP Unreachable message, it con-</td>
</tr>
</tbody>
</table>
siders the targeted host dead. This approach helps speed up discovery on some networks.

**Note:** Some firewalls and packet filters use this same behavior for hosts that are up, but connected to a port or protocol that is filtered. With this option enabled, this leads to the scan considering the host is down when it is indeed up.

<table>
<thead>
<tr>
<th><strong>UDP</strong></th>
<th><strong>Disabled</strong></th>
<th>Ping a host using the User Datagram Protocol (UDP). UDP is a stateless protocol, meaning that communication is not performed with handshake dialogues. UDP-based communication is not always reliable, and because of the nature of UDP services and screening devices, they are not always remotely detectable.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximum Number of Retries</strong></td>
<td><strong>2</strong></td>
<td>Specifies the number of attempts to retry pinging the remote host.</td>
</tr>
</tbody>
</table>

**Fragile Devices**

| **Scan Network Printers** | **Disabled** | When enabled, the scanner scans network printers. |
| **Scan Novell Netware Hosts** | **Disabled** | When enabled, the scanner scans Novell NetWare hosts. |
| **Scan Operational Technology Devices** | **Disabled** | When enabled, the scanner performs a full scan of Operational Technology (OT) devices such as programmable logic controllers (PLCs) and remote terminal units (RTUs) that monitor environmental factors and the activity and state of machinery. When disabled, the scanner uses ICS/SCADA Smart Scanning to cautiously identify OT devices and stops scanning them once they are discovered. |

**Wake-on-LAN**

| **List of** | **None** | The Wake-on-LAN (WOL) menu controls which hosts |
MAC Addresses to send WOL magic packets to before performing a scan.

Hosts that you want to start prior to scanning are provided by uploading a text file that lists one MAC address per line.

For example:

```
33:24:4C:03:CC:C7
FF:5C:2C:71:57:79
```

Boot Time Wait (In Minutes) 5 minutes The amount of time to wait for hosts to start before performing the scan.

Port Scanning

The Port Scanning section includes settings that define how the port scanner behaves and which ports to scan.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consider Unscanned Ports as Closed</td>
<td>Disabled</td>
<td>When enabled, if a port is not scanned with a selected port scanner (for example, the port falls outside of the specified range), the scanner considers it closed.</td>
</tr>
<tr>
<td>Port Scan Range</td>
<td>Default</td>
<td>Specifies the range of ports to be scanned. Supported keyword values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- default instructs the scanner to scan approximately 4,790 commonly used ports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- all instructs the scanner to scan all 65,536 ports, including port 0.</td>
</tr>
</tbody>
</table>
Additionally, you can indicate a custom list of ports by using a comma-delimited list of ports or port ranges. For example, `21,23,25,80,110 or 1-1024,8080,9000-9200`. If you wanted to scan all ports excluding port 0, you would type `1-65535`.

The custom range specified for a port scan is applied to the protocols you have selected in the **Network Port Scanners** group of settings.

If scanning both TCP and UDP, you can specify a split range specific to each protocol. For example, if you want to scan a different range of ports for TCP and UDP in the same policy, you would type `T:1-1024,U:300-500`.

You can also specify a set of ports to scan for both protocols, as well as individual ranges for each separate protocol. For example, `1-1024,T:1024-65535,U:1025`.

You can also include `default` in a list of custom ports. For example, `T:64999,default,U:55550-55555`.

### Local Port Enumerators

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH (netstat)</td>
<td>Enabled</td>
<td>When enabled, the scanner uses <code>netstat</code> to check for open ports from the local machine. It relies on the <code>netstat</code> command being available via an SSH connection to the target. This scan is intended for Linux-based systems and requires authentication credentials.</td>
</tr>
<tr>
<td>WMI (netstat)</td>
<td>Enabled</td>
<td>When enabled, the scanner uses <code>netstat</code> to determine open ports while performing a WMI-based scan. In addition, the scanner:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Ignores any custom range specified in the <strong>Port Scan</strong></td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Range setting.</strong></td>
<td></td>
<td><strong>Continues to treat unscanned ports as closed</strong> if the <strong>Consider unscanned ports as closed</strong> setting is enabled. If any port enumerator (netstat or SNMP) is successful, the port range becomes <em>all</em>.</td>
</tr>
<tr>
<td><strong>SNMP</strong></td>
<td>Enabled</td>
<td>When enabled, if the appropriate credentials are provided by the user, the scanner can better test the remote host and produce more detailed audit results. For example, there are many Cisco router checks that determine the vulnerabilities present by examining the version of the returned SNMP string. This information is necessary for these audits.</td>
</tr>
<tr>
<td>Only Run Network Port Scanners if Local Port Enumeration Failed</td>
<td>Enabled</td>
<td>When enabled, the scanner relies on local port enumeration first before relying on network port scans.</td>
</tr>
<tr>
<td>Verify Open TCP Ports Found By Local Port Enumerators</td>
<td>Disabled</td>
<td>When enabled, if a local port enumerator (for example, WMI or netstat) finds a port, the scanner also verifies that the port is open remotely. This approach helps determine if some form of access control is being used (for example, TCP wrappers or a firewall).</td>
</tr>
<tr>
<td><strong>Network Port Scanners</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>Disabled</td>
<td>Use the built-in Nessus TCP scanner to identify open TCP ports on the targets, using a full TCP three-way handshake. TCP scans are only possible if you are using Linux or FreeBSD. On Windows or Mac OS X, the scanner does</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SYN</td>
<td>Enabled</td>
<td>Use the built-in Nessus SYN scanner to identify open TCP ports on the target hosts. SYN scans do not initiate a full TCP three-way handshake. The scanner sends a SYN packet to the port, waits for SYN-ACK reply, and determines the port state based on a response or lack of response. If you enable this option, you can also set the <strong>Override Automatic Firewall Detection</strong> option.</td>
</tr>
</tbody>
</table>
| Override Automatic Firewall Detection            | Disabled      | This setting can be enabled if you enable either the TCP or SYN option. When enabled, this setting overrides automatic firewall detection. This setting has three options:  
  - **Use aggressive detection** attempts to run plugins even if the port appears to be closed. It is recommended that this option not be used on a production network.  
  - **Use soft detection** disables the ability to monitor how often resets are set and to determine if there is a limitation configured by a downstream network device.  
  - **Disable detection** disables the firewall detection fea- |
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>This description also applies to the <strong>Override automatic firewall detection</strong> setting that is available following SYN.</td>
</tr>
<tr>
<td>UDP</td>
<td>Disabled</td>
<td>This option engages the built-in Nessus UDP scanner to identify open UDP ports on the targets. Due to the nature of the protocol, it is generally not possible for a port scanner to tell the difference between open and filtered UDP ports. Enabling the UDP port scanner may dramatically increase the scan time and produce unreliable results. Consider using the netstat or SNMP port enumeration options instead if possible.</td>
</tr>
</tbody>
</table>

### Service Discovery

The **Service Discovery** section includes settings that attempt to map each open port with the service that is running on that port.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Probe All Ports to Find Services</td>
<td>Enabled</td>
<td>When enabled, the scanner attempts to map each open port with the service that is running on that port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Caution:</strong> In some rare cases, probing might disrupt some services and cause unforeseen side effects.</td>
</tr>
<tr>
<td>Search for SSL/TLS Based Services</td>
<td>On</td>
<td>Controls how the scanner tests SSL-based services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Caution:</strong> Testing for SSL capability on all ports may be disruptive for the tested host.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Search for SSL/TLS Services (enabled)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Search for SSL/TLS On                       | Known SSL/TLS ports | Specifies which ports on target hosts the scanner searches for SSL/TLS services. This setting has two options:  
- Known SSL/TLS ports  
- All TCP ports |
| Identify Certificates Expiring Within x Days | 60            | When enabled, the scanner identifies SSL and TLS certificates that are within the specified number of days of expiring.                                                                                      |
| Enumerate All SSL/TLS Ciphers               | True          | When enabled, the scanner ignores the list of ciphers advertised by SSL/TLS services and enumerates them by attempting to establish connections using all possible ciphers. |
| Enable CRL Checking (Connects to the Internet) | False        | When enabled, the scanner checks that none of the identified certificates have been revoked.                                                                                                                     |
## Preconfigured Discovery Settings

Certain Tenable-provided scanner templates include preconfigured discovery settings, described in the following table. The preconfigured discovery settings are determined by both the template and the **Scan Type** that you select.

<table>
<thead>
<tr>
<th>Template</th>
<th>Scan Type</th>
<th>Preconfigured Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerability Scans (Common)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Advanced Network Scan</strong></td>
<td>-</td>
<td><strong>All defaults</strong></td>
</tr>
<tr>
<td><strong>Basic Network Scan</strong></td>
<td>Port scan (common ports) (default)</td>
<td>- General Settings:&lt;br&gt;◦ Always test the local Nessus host&lt;br&gt;◦ Port Scanner Settings:&lt;br&gt;◦ Scan common ports&lt;br&gt;◦ Use netstat if credentials are provided&lt;br&gt;◦ Use SYN scanner if necessary&lt;br&gt;◦ Ping hosts using:&lt;br&gt;◦ TCP&lt;br&gt;◦ ARP&lt;br&gt;◦ ICMP (2 retries)</td>
</tr>
<tr>
<td><strong>Port scan</strong> (all ports)</td>
<td></td>
<td>- General Settings:&lt;br&gt;◦ Always test the local Nessus host&lt;br&gt;◦ Port Scanner Settings:</td>
</tr>
</tbody>
</table>
### Custom

<table>
<thead>
<tr>
<th>Credentialed Patch Audit</th>
<th>Port scan (common ports) (default)</th>
<th>Port scan (all ports)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan all ports (1-65535)</td>
<td>Use netstat if credentials are provided</td>
<td>General Settings:</td>
</tr>
<tr>
<td>Use SYN scanner if necessary</td>
<td>Ping hosts using:</td>
<td>○ Always test the local Nessus host</td>
</tr>
<tr>
<td>• Ping hosts using:</td>
<td>○ TCP</td>
<td>○ Port Scanner Settings:</td>
</tr>
<tr>
<td>○ TCP</td>
<td>○ ARP</td>
<td>○ Scan common ports</td>
</tr>
<tr>
<td>○ ARP</td>
<td>○ ICMP (2 retries)</td>
<td>○ Use netstat if credentials are provided</td>
</tr>
<tr>
<td>○ ICMP (2 retries)</td>
<td></td>
<td>○ Use SYN scanner if necessary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ping hosts using:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ TCP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ ARP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>○ ICMP (2 retries)</td>
</tr>
</tbody>
</table>

---

**All defaults**
<table>
<thead>
<tr>
<th>Custom</th>
<th>All defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host Discovery</strong></td>
<td><strong>Host enumeration</strong> (default)</td>
</tr>
<tr>
<td></td>
<td>• General Settings:</td>
</tr>
<tr>
<td></td>
<td>o Always test the local Nessus host</td>
</tr>
<tr>
<td></td>
<td>o Ping hosts using:</td>
</tr>
<tr>
<td></td>
<td>o TCP</td>
</tr>
<tr>
<td></td>
<td>o ARP</td>
</tr>
<tr>
<td></td>
<td>o ICMP (2 retries)</td>
</tr>
<tr>
<td></td>
<td>• General Settings:</td>
</tr>
<tr>
<td></td>
<td>o Always test the local Nessus host</td>
</tr>
<tr>
<td></td>
<td>o Ping hosts using:</td>
</tr>
<tr>
<td></td>
<td>o TCP</td>
</tr>
<tr>
<td></td>
<td>o ARP</td>
</tr>
<tr>
<td></td>
<td>o ICMP (2 retries)</td>
</tr>
</tbody>
</table>

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable,Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
| Port scan (common ports) | General Settings:  
| | ◦ Always test the local Nessus host  
| | Port Scanner Settings:  
| | ◦ Scan common ports  
| | ◦ Use netstat if credentials are provided  
| | ◦ Use SYN scanner if necessary  
| | Ping hosts using:  
| | ◦ TCP  
| | ◦ ARP  
| | ◦ ICMP (2 retries)  
| Port scan (all ports) | General Settings:  
| | ◦ Always test the local Nessus host  
| | Port Scanner Settings:  
| | ◦ Scan all ports (1-65535)  
| | ◦ Use netstat if credentials are provided  
<p>| | ◦ Use SYN scanner if necessary |</p>
<table>
<thead>
<tr>
<th><strong>Custom</strong></th>
<th><strong>All defaults</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal PCI Network Scan</strong></td>
<td><strong>Port scan (common ports)</strong> (default)</td>
</tr>
<tr>
<td>necessary</td>
<td></td>
</tr>
<tr>
<td>• Ping hosts using:</td>
<td></td>
</tr>
<tr>
<td>◦ TCP</td>
<td></td>
</tr>
<tr>
<td>◦ ARP</td>
<td></td>
</tr>
<tr>
<td>◦ ICMP (2 retries)</td>
<td></td>
</tr>
<tr>
<td><strong>Port scan (all ports)</strong></td>
<td><strong>General Settings:</strong></td>
</tr>
<tr>
<td></td>
<td>◦ Always test the local Nessus host</td>
</tr>
<tr>
<td></td>
<td><strong>Port Scanner Settings:</strong></td>
</tr>
<tr>
<td></td>
<td>◦ Scan common ports</td>
</tr>
<tr>
<td></td>
<td>◦ Use netstat if credentials are provided</td>
</tr>
<tr>
<td></td>
<td>◦ Use SYN scanner if necessary</td>
</tr>
<tr>
<td></td>
<td><strong>Ping hosts using:</strong></td>
</tr>
<tr>
<td></td>
<td>◦ TCP</td>
</tr>
<tr>
<td></td>
<td>◦ ARP</td>
</tr>
<tr>
<td></td>
<td>◦ ICMP (2 retries)</td>
</tr>
<tr>
<td></td>
<td><strong>General Settings:</strong></td>
</tr>
<tr>
<td></td>
<td>◦ Always test the local Nessus host</td>
</tr>
<tr>
<td></td>
<td><strong>Port Scanner Settings:</strong></td>
</tr>
<tr>
<td></td>
<td>◦ Scan all ports (1-65535)</td>
</tr>
<tr>
<td>Custom</td>
<td>All defaults</td>
</tr>
<tr>
<td>--------</td>
<td>--------------</td>
</tr>
<tr>
<td><strong>Legacy Web App Scan</strong></td>
<td><strong>Port scan (common ports)</strong> (default)</td>
</tr>
</tbody>
</table>

- Use `netstat` if credentials are provided
- Use `SYN` scanner if necessary

- Ping hosts using:
  - TCP
  - ARP
  - ICMP (2 retries)

- **General Settings:**
  - Always test the local Nessus host

- **Port Scanner Settings:**
  - Scan common ports
  - Use `netstat` if credentials are provided
  - Use `SYN` scanner if necessary

- Ping hosts using:
  - TCP
  - ARP
  - ICMP (2 retries)

- **General Settings:**
  - Always test the local Nessus host
<table>
<thead>
<tr>
<th>Policy Compliance Auditing</th>
<th>Default (default)</th>
<th>General Settings:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Ping the remote host</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Always test the local Nessus host</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Scan all devices, including:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Mobile Device Scan</strong></th>
<th>Custom</th>
<th>All defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PCI Quarterly External Scan</strong></td>
<td>-</td>
<td>Scan unresponsive hosts default</td>
</tr>
<tr>
<td><strong>Configuration Scans</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Audit Cloud Infrastructure</strong></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td><strong>MDM Config Audit</strong></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td><strong>Offline Config Audit</strong></td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

### Port Scanner Settings:
- Scan all ports (1-65535)
- Use netstat if credentials are provided
- Use SYN scanner if necessary

### Ping hosts using:
- TCP
- ARP
- ICMP (2 retries)
<table>
<thead>
<tr>
<th>SCAP and OVAL Auditing</th>
<th>Custom</th>
<th>All defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host enumeration (default)</td>
<td>Host enumeration (default)</td>
<td>Host enumeration (default)</td>
</tr>
<tr>
<td>General Settings:</td>
<td>General Settings:</td>
<td>General Settings:</td>
</tr>
<tr>
<td>- Always test the local Nessus host</td>
<td>- Always test the local Nessus host</td>
<td>- Always test the local Nessus host</td>
</tr>
<tr>
<td>- Ping hosts using:</td>
<td>- Ping hosts using:</td>
<td>- Ping hosts using:</td>
</tr>
<tr>
<td>- TCP</td>
<td>- TCP</td>
<td>- TCP</td>
</tr>
<tr>
<td>- ARP</td>
<td>- ARP</td>
<td>- ARP</td>
</tr>
<tr>
<td>- ICMP (2 retries)</td>
<td>- ICMP (2 retries)</td>
<td>- ICMP (2 retries)</td>
</tr>
<tr>
<td>Custom</td>
<td>Custom</td>
<td>Custom</td>
</tr>
<tr>
<td>All defaults</td>
<td>All defaults</td>
<td>All defaults</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tactical Scans</th>
<th>Tactical Scans</th>
<th>Tactical Scans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Badlock Detection</td>
<td>Quick</td>
<td>Normal (default)</td>
</tr>
<tr>
<td>Quick</td>
<td>Quick</td>
<td>Normal (default)</td>
</tr>
<tr>
<td>General Settings:</td>
<td>General Settings:</td>
<td>General Settings:</td>
</tr>
<tr>
<td>- Ping the remote host</td>
<td>- Ping the remote host</td>
<td>- Ping the remote host</td>
</tr>
<tr>
<td>- Always test the local Nessus host</td>
<td>- Always test the local Nessus host</td>
<td>- Always test the local Nessus host</td>
</tr>
<tr>
<td>Service Discovery Settings:</td>
<td>Service Discovery Settings:</td>
<td>Service Discovery Settings:</td>
</tr>
<tr>
<td>- Scan TCP ports 23, 25, 80, and 443</td>
<td>- Scan TCP ports 23, 25, 80, and 443</td>
<td>- Scan TCP ports 23, 25, 80, and 443</td>
</tr>
<tr>
<td>- Detect SSL/TLS on ports where it is commonly used</td>
<td>- Detect SSL/TLS on ports where it is commonly used</td>
<td>- Detect SSL/TLS on ports where it is commonly used</td>
</tr>
</tbody>
</table>

- Printers
- Novell Netware hosts
### Thorough

- **General Settings:**
  - Ping the remote host
  - Always test the local Nessus host

- **Service Discovery Settings:**
  - Scan all TCP ports
  - Detect SSL on all open ports

---

### Custom

- **General Settings:**
  - Ping the remote host
  - Always test the local Nessus host

- **Service Discovery Settings:**
  - Scan the default Nessus port range
  - Detect SSL/TLS on ports where it is commonly used

---

### Quick

- **General Settings:**
  - Ping the remote host
  - Always test the local Nessus host

- **Service Discovery Settings:**
  - Scan TCP ports 23, 25, 80, and 443
  - Detect SSL/TLS on ports where it is commonly used
<table>
<thead>
<tr>
<th><strong>Normal</strong> (default)</th>
<th><strong>Thorough</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Scan all devices, including:</td>
<td>- Scan all devices, including:</td>
</tr>
<tr>
<td>◦ Printers</td>
<td>◦ Printers</td>
</tr>
<tr>
<td>◦ Novell Netware hosts</td>
<td>◦ Novell Netware hosts</td>
</tr>
</tbody>
</table>

**Normal** (default) Settings:
- General Settings:
  ◦ Ping the remote host
  ◦ Always test the local Nessus host
- Service Discovery Settings:
  ◦ Scan the default Nessus port range
  ◦ Detect SSL/TLS on ports where it is commonly used

**Thorough** Settings:
- General Settings:
  ◦ Ping the remote host
  ◦ Always test the local Nessus host
- Service Discovery Settings:
  ◦ Scan all TCP ports
  ◦ Detect SSL on all open ports
- Scan all devices, including:
<table>
<thead>
<tr>
<th>Custom</th>
<th>All defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DROWN Detection</strong></td>
<td><strong>Quick</strong></td>
</tr>
<tr>
<td></td>
<td>• General Settings:</td>
</tr>
<tr>
<td></td>
<td>◦ Ping the remote host</td>
</tr>
<tr>
<td></td>
<td>◦ Always test the local Nessus host</td>
</tr>
<tr>
<td></td>
<td>• Service Discovery Settings:</td>
</tr>
<tr>
<td></td>
<td>◦ Scan TCP ports 23, 25, 80, and 443</td>
</tr>
<tr>
<td></td>
<td>◦ Detect SSL/TLS on ports where it is commonly used</td>
</tr>
<tr>
<td>Normal (default)</td>
<td>• General Settings:</td>
</tr>
<tr>
<td></td>
<td>◦ Ping the remote host</td>
</tr>
<tr>
<td></td>
<td>◦ Always test the local Nessus host</td>
</tr>
<tr>
<td></td>
<td>• Service Discovery Settings:</td>
</tr>
<tr>
<td></td>
<td>◦ Scan the default Nessus port range</td>
</tr>
<tr>
<td></td>
<td>◦ Detect SSL/TLS on ports where it is commonly used</td>
</tr>
<tr>
<td>Thorough</td>
<td>• General Settings:</td>
</tr>
<tr>
<td></td>
<td>◦ Ping the remote host</td>
</tr>
<tr>
<td></td>
<td>◦ Always test the local</td>
</tr>
</tbody>
</table>
### Service Discovery Settings:
- **Scan all TCP ports**
- **Detect SSL on all open ports**

<table>
<thead>
<tr>
<th>Custom</th>
<th>All defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intel AMT Security Bypass</strong></td>
<td><strong>Quick</strong></td>
</tr>
</tbody>
</table>

- **General Settings:**
  - Ping the remote host
  - Always test the local Nessus host
- **Service Discovery Settings:**
  - Scan TCP ports 16992, 16993, 623, 80, and 443
  - Detect SSL/TLS on ports where it is commonly used

<table>
<thead>
<tr>
<th><strong>Normal</strong> (default)</th>
<th><strong>Normal</strong> (default)</th>
</tr>
</thead>
</table>

- **General Settings:**
  - Ping the remote host
  - Always test the local Nessus host
- **Service Discovery Settings:**
  - Scan the default Nessus port range
  - Detect SSL/TLS on ports where it is commonly used
<table>
<thead>
<tr>
<th>Malware Scan</th>
<th>Host enumeration (default)</th>
<th>Host enumeration (include fragile hosts)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Thorough</strong></td>
<td>• General Settings:</td>
<td>• General Settings:</td>
</tr>
<tr>
<td></td>
<td>◦ Ping the remote host</td>
<td>◦ Always test the local Nessus host</td>
</tr>
<tr>
<td></td>
<td>◦ Always test the local</td>
<td>◦ Ping hosts using:</td>
</tr>
<tr>
<td></td>
<td>Nessus host</td>
<td>◦ TCP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ ARP</td>
</tr>
<tr>
<td></td>
<td>• Service Discovery Settings:</td>
<td>◦ Detect SSL on all open ports</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Custom</strong></td>
<td><strong>All defaults</strong></td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective
<table>
<thead>
<tr>
<th>Shadow Brokers Scan</th>
<th>Normal (default)</th>
<th>Thorough</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>General Settings:</strong></td>
<td><strong>General Settings:</strong></td>
</tr>
<tr>
<td></td>
<td>◦ Ping the remote host</td>
<td>◦ Ping the remote host</td>
</tr>
<tr>
<td></td>
<td>◦ Always test the local Nessus host</td>
<td>◦ Always test the local Nessus host</td>
</tr>
<tr>
<td></td>
<td><strong>Service Discovery Settings:</strong></td>
<td><strong>Service Discovery Settings:</strong></td>
</tr>
<tr>
<td></td>
<td>◦ Scan the default Nessus port range</td>
<td>◦ Scan all TCP ports</td>
</tr>
<tr>
<td></td>
<td>◦ Detect SSL/TLS on ports where it is commonly used</td>
<td>◦ Detect SSL on all open ports</td>
</tr>
<tr>
<td></td>
<td><strong>Scan all devices, including:</strong></td>
<td><strong>Scan all devices, including:</strong></td>
</tr>
<tr>
<td></td>
<td>◦ Printers</td>
<td>◦ Printers</td>
</tr>
<tr>
<td></td>
<td>◦ Novell Netware hosts</td>
<td>◦ Novell Netware hosts</td>
</tr>
</tbody>
</table>

**Custom**

**All defaults**
<table>
<thead>
<tr>
<th>Detection Type</th>
<th>Scan Options</th>
<th>General Settings</th>
<th>Service Discovery Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spectre and Meltdown Detection</td>
<td>Normal (default)</td>
<td>Ping the remote host</td>
<td>Scan the default Nessus port range</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Always test the local Nessus host</td>
<td>Detect SSL/TLS on ports where it is commonly used</td>
</tr>
<tr>
<td></td>
<td>Custom</td>
<td>All defaults</td>
<td></td>
</tr>
<tr>
<td>WannaCry Ransomware Detection</td>
<td>Quick</td>
<td>General Settings:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ping the remote host</td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td>Normal (default)</td>
<td>Thorough</td>
<td>Custom</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
</tbody>
</table>
| Always test the local Nessus host | • Service Discovery Settings:  
  ◦ Scan TCP ports 139 and 445  
  ◦ Detect SSL/TLS on ports where it is commonly used | • General Settings:  
  ◦ Ping the remote host  
  ◦ Always test the local Nessus host  
  • Service Discovery Settings:  
  ◦ Scan the default Nessus port range  
  ◦ Detect SSL/TLS on ports where it is commonly used |        |               |
|                    | • General Settings:  
  ◦ Ping the remote host  
  ◦ Always test the local Nessus host | • General Settings:  
  ◦ Ping the remote host  
  ◦ Always test the local Nessus host  
  • Service Discovery Settings:  
  ◦ Scan all TCP ports  
  ◦ Detect SSL on all open ports |        |               |
Scope Settings in WAS Scans

Configure Scope settings to specify the URLs and file types that you want to include in or exclude from your scan.

You can configure Scope settings when you create a scan or user-defined scan template and select the Overview or Scan template type. For more information, see Scan Templates.

Tip: If you want to save your settings configurations and apply them to other scans, you can create and configure a user-defined scan template.

The Scope settings include the following sections:

- **Crawl Scripts**
- **OpenAPI (Swagger) Specification**
- **Scan Inclusion**
- **Scan Exclusion**

Crawl Scripts

Selenium scripts you want to add to your scan to enable the scanner to analyze pages with complex access logic.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Add File    | Hyperlink that allows you to add one or more recorded Selenium script files to your scan.  
Your script must be added as a .side file.  |

OpenAPI (Swagger) Specification

The specification file for the RESTful API that you want to scan. The file should be OpenAPI Specification (v2 or v3) compliant and represented in either JSON or YAML format.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add File</td>
<td>Hyperlink that allows you to add one or more OpenAPI (v2 or v3) specification</td>
</tr>
</tbody>
</table>
files. The specification files should be represented in either JSON or YAML format.

### Scan Inclusion

The URLs you want the scanner to include, along with how you want the scanner to crawl them.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of URLs</td>
<td>none</td>
<td>A list of any URLs you want to ensure the scanner analyzes, in addition to the target URL you specified in the Basic settings. Type each URL as an absolute URL. Type each URL on a separate line.</td>
</tr>
</tbody>
</table>
| Specify how the scanner handles URLs found during the application crawl | Crawl all URLs detected | Specifies the limits you want the scanner to adhere to as it crawls URLs. Select one of the following:  
  - **Crawl all URLs detected** – The scanner crawls all URLs and child paths it detects on the target URL’s domain host.  
  - **Limit crawling to specified URLs and child paths** – The scanner crawls only the target URL and child paths.  
  - **Limit crawling to specified URLs** – The scanner crawls the target URL only. It does not crawl child paths for the target URL. |

### Scan Exclusion
The attributes of URLs you want the scanner to exclude from your scan.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regex for Excluded URLs</td>
<td>logout</td>
<td>Text box option in which you can specify a regex pattern that the scanner can look for in URLs to exclude from the scan. You can specify multiple regex patterns separated by new lines.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The regex values should be values contained within the URL to be excluded. For example, in the URL <code>http://www.example.com/blog/today.htm</code>, valid regex values would be blog or today (not the full URL). Additionally, regex values are case-sensitive.</td>
</tr>
<tr>
<td>File Extensions to Exclude</td>
<td>js, css, png, jpeg, gif, pdf, csv, svn-base, svg, jpg, ico</td>
<td>Text box option in which you can specify the file types you want the scanner to exclude from the scan. Separate each file type with a comma.</td>
</tr>
<tr>
<td>Decompose Paths</td>
<td>not selected</td>
<td>Check box option that allows you to specify whether you want the scanner to break down each URL identified during the scan into additional URLs, based on directory path level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, if you specify <code>www.example.com/dir1/dir2/dir3</code> as your target and select <strong>Decompose Paths</strong>, the scanner analyzes each of the following as separate URLs of the target:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>www.example.com/dir1/dir2/dir3</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>www.example.com/dir1/dir2</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>www.example.com/dir1</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select this option to increase the surface coverage of your web application scan.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong>: Scans that include path decomposition can take longer to complete than scans that do not.</td>
</tr>
</tbody>
</table>
Assessment Settings in Vulnerability Management Scans

**Note:** If a scan is based on a user-defined template, you cannot configure Assessment settings in the scan. You can only modify these settings in the related user-defined template.

You can use Assessment settings to configure how a scan identifies vulnerabilities, as well as what vulnerabilities are identified. This includes identifying malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility of web applications.

Certain Tenable-provided scanner templates include preconfigured assessment settings.

If you select the Custom preconfigured setting option, or if you are using a scanner template that does not include preconfigured assessment settings, you can manually configure Assessment settings in the following categories:

- **General**
- **Brute Force**
- **SCADA**
- **Web Applications**
- **Windows**
- **Malware**
- **Databases**

**Note:** The following tables include settings for the Advanced Network Scan template. Depending on the template you select, certain settings may not be available, and default values may vary.

**General**

The General section includes the following groups of settings:

- **Accuracy**
- **Antivirus**
- **SMTP**
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accuracy</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Override Normal Accuracy</td>
<td>Disabled</td>
<td>In some cases, Tenable.io cannot remotely determine whether a flaw is present or not. If report paranoia is set to <strong>Show potential false alarms</strong>, a flaw is reported every time, even when there is a doubt about the remote host being affected. Conversely, a paranoia setting of <strong>Avoid potential false alarms</strong> causes Tenable.io to not report any flaw whenever there is a hint of uncertainty about the remote host. As a middle ground between these two settings, disable this setting.</td>
</tr>
<tr>
<td><strong>Perform thorough tests</strong></td>
<td>Disabled</td>
<td>Causes various plugins to work harder. For example, when looking through SMB file shares, a plugin analyzes 3 directory levels deep instead of 1. This could cause much more network traffic and analysis in some cases. By being more thorough, the scan is more intrusive and is more likely to disrupt the network, while potentially providing better audit results.</td>
</tr>
<tr>
<td><strong>Antivirus</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antivirus definition grace period (in days)</td>
<td>0</td>
<td>Configure the delay of the Antivirus software check for a set number of days (0-7). The Antivirus Software Check menu allows you to direct Tenable.io to allow for a specific grace time in reporting when antivirus signatures are considered out of date. By default, Tenable.io considers signatures out of date regardless of how long ago an update became available (e.g., a few hours ago). You can configure this option to allow for up to 7 days before reporting them out of date.</td>
</tr>
<tr>
<td><strong>SMTP</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third party domain</td>
<td>Tenable.io attempts to send spam through each SMTP device to the address listed in this field. This third party domain address must be outside the range of</td>
<td></td>
</tr>
</tbody>
</table>
the site being scanned or the site performing the scan. Otherwise, the test may be aborted by the SMTP server.

<table>
<thead>
<tr>
<th>From address</th>
<th>The test messages sent to the SMTP server(s) appear as if the messages originated from the address specified in this field.</th>
</tr>
</thead>
<tbody>
<tr>
<td>To address</td>
<td>Tenable.io attempts to send messages addressed to the mail recipient listed in this field. The postmaster address is the default value since it is a valid address on most mail servers.</td>
</tr>
</tbody>
</table>

**Brute Force**

The **Brute Force** section includes the following groups of settings:

- [General Settings](#)
- [Oracle Database](#)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Only use credentials provided by the user</td>
<td>Enabled</td>
<td>In some cases, Tenable.io can test default accounts and known default passwords. This can cause the account to be locked out if too many consecutive invalid attempts trigger security protocols on the operating system or application. By default, this setting is enabled to prevent Tenable.io from performing these tests.</td>
</tr>
<tr>
<td><strong>Oracle Database</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test default accounts (slow)</td>
<td>Disabled</td>
<td>Test for known default accounts in Oracle software.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Modbus/TCP Coil Access</td>
<td></td>
<td>Modbus uses a function code of 1 to read coils in a Modbus slave. Coils represent binary output settings and are typically mapped to actuators. The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a write coil message.</td>
</tr>
<tr>
<td>Start at Register</td>
<td>0</td>
<td>The register at which to start scanning.</td>
</tr>
<tr>
<td>End at Register</td>
<td>16</td>
<td>The register at which to stop scanning.</td>
</tr>
<tr>
<td>ICCP/COTP TSAP Addressing Weakness</td>
<td></td>
<td>The ICCP/COTP TSAP Addressing menu determines a Connection Oriented Transport Protocol (COTP) Transport Service Access Points (TSAP) value on an ICCP server by trying possible values.</td>
</tr>
<tr>
<td>Start COTP TSAP</td>
<td>8</td>
<td>Specifies the starting TSAP value to try. Tenable.io tries all values between the Start and Stop values.</td>
</tr>
<tr>
<td>Stop COTP TSAP</td>
<td>8</td>
<td>Specifies the ending TSAP value to try. Tenable.io tries all values between the Start and Stop values.</td>
</tr>
</tbody>
</table>

### Web Applications

The **Web Applications** section includes the following groups of settings:

- [General Settings](#)
- [Web Crawler](#)
- [Application Test Settings](#)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan web applications</td>
<td>Disabled</td>
<td>By default, Tenable.io does not scan web applications. To edit the following settings,</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use a custom User-Agent</td>
<td>Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)</td>
<td>Specifies which type of web browser Tenable.io impersonates while scanning.</td>
</tr>
<tr>
<td><strong>Web Crawler</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start crawling from</td>
<td>/</td>
<td>The URL of the first page that is tested. If multiple pages are required, use a colon delimiter to separate them (e.g., /://php-p4://base).</td>
</tr>
<tr>
<td>Excluded pages (regex)</td>
<td>/server_privileges.php &lt;&gt; log out</td>
<td>Specifies portions of the web site to exclude from being crawled. For example, to exclude the /manual directory and all Perl CGI, set this field to: (^/manual) &lt;&gt; (.pl (.?.*)?$). Tenable.io supports POSIX regular expressions for string matching and handling, as well as Perl-compatible regular expressions (PCRE).</td>
</tr>
<tr>
<td>Maximum pages to crawl</td>
<td>1000</td>
<td>The maximum number of pages to crawl.</td>
</tr>
<tr>
<td>Maximum depth to crawl</td>
<td>6</td>
<td>Limit the number of links Tenable.io follows for each start page.</td>
</tr>
<tr>
<td>Follow dynamically generated pages</td>
<td>Disabled</td>
<td>If selected, Tenable.io follows dynamic links and may exceed the parameters set above.</td>
</tr>
<tr>
<td><strong>Application Test Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable generic web application tests</td>
<td>Disabled</td>
<td>Enables the following settings.</td>
</tr>
<tr>
<td>Abort web application tests if HTTP login fails</td>
<td>Disabled</td>
<td>If Tenable.io cannot log in to the target via HTTP, then do not run any web application tests.</td>
</tr>
<tr>
<td>Try all HTTP methods</td>
<td>Disabled</td>
<td>This option instructs Tenable.io to also use POST requests for enhanced web form testing. By default, the web application tests only use GET requests, unless you enable this option. Generally, more complex applications use the POST method when a user submits data to the application. When enabled, Tenable.io tests each script or variable with both GET and POST requests. This setting provides more thorough testing, but may considerably increase the time required.</td>
</tr>
<tr>
<td>Attempt HTTP Parameter Pollution</td>
<td>Disabled</td>
<td>When performing web application tests, attempt to bypass filtering mechanisms by injecting content into a variable while also supplying the same variable with valid content. For example, a normal SQL injection test may look like /target.cgi?a='&amp;b=2. With HTTP Parameter Pollution (HPP) enabled, the request may look like /target.cgi?a='&amp;a=1&amp;b=2.</td>
</tr>
<tr>
<td>Test embedded web servers</td>
<td>Disabled</td>
<td>Embedded web servers are often static and contain no customizable CGI scripts. In</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Test more than one parameter at a time perform</td>
<td>Disabled</td>
<td>This setting manages the combination of argument values used in the HTTP requests. The default, without checking this option, is testing one parameter at a time with an attack string, without trying non-attack variations for additional parameters. For example, Tenable.io would attempt /test.php?arg1=XSS&amp;b=1&amp;c=1, where b and c allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This setting has four options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Test random pairs of parameters</strong>: This form of testing randomly checks a combination of random pairs of parameters. This is the fastest way to test multiple parameters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Test all pairs of parameters (slow)</strong>: This form of testing is slightly slower but more efficient than the one value test. While testing multiple parameters, it tests an attack string, variations for a single variable and then use the first value for all other vari-</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ables. For example, Tenable.io would attempt <code>/test.php?a-a=XSS&amp;a=1&amp;b=1&amp;c=1&amp;d=1</code> and then cycle through the variables so that one is given the attack string, one is cycled through all possible values (as discovered during the mirror process) and any other variables are given the first value. In this case, Tenable.io would never test for <code>/test.php?a-a=XSS&amp;a=3&amp;b=3&amp;c=3&amp;d=3</code> when the first value of each variable is 1.</td>
</tr>
</tbody>
</table>

- **Test random combinations of three or more parameters (slower):** This form of testing randomly checks a combination of three or more parameters. This is more thorough than testing only pairs of parameters. Increasing the amount of combinations by three or more increases the web application test time.

- **Test all combinations of parameters (slowest):** This method of testing checks all possible combinations of attack strings with valid input to variables. Where all pairs testing seeks to create a smaller data set as a tradeoff for speed, all combinations makes no compromise on time and uses a complete data set of tests. This testing method may take a long time to com-
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not stop after first flaw is found per web page</td>
<td>Stop after one flaw is found per web server (fastest)</td>
<td>This setting determines when a new flaw is targeted. This applies at the script level. Finding an XSS flaw does not disable searching for SQL injection or header injection, but unless otherwise specified, there is at most one report for each type on a given port. Note that several flaws of the same type (for example, XSS or SQLi) may be reported if they were caught by the same attack.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If this option is disabled, as soon as a flaw is found on a web page, the scan moves on to the next web page. If you enable this option, select one of the following options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Stop after one flaw is found per web server (fastest)</strong> – (Default) As soon as a flaw is found on a web server by a script, Tenable.io stops and switches to another web server on a different port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Stop after one flaw is found per parameter (slow)</strong> – As soon as one type of flaw is found in a parameter of a CGI (for example, XSS), Tenable.io switches to the next parameter of the same CGI, the next known CGI, or to the next port or server.</td>
</tr>
</tbody>
</table>

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
### Setting

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Look for all flaws (slowest)</strong> – Perform extensive tests regardless of flaws found. This option can produce a very verbose report and is not recommend in most cases.**</td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL for Remote File Inclusion</td>
<td><a href="http://rfi.nessus.org/rfi.txt">http://rfi.nessus.org/rfi.txt</a></td>
<td>During Remote File Inclusion (RFI) testing, this setting specifies a file on a remote host to use for tests. By default, Tenable.io uses a safe file hosted by Tenable for RFI testing. If the scanner cannot reach the Internet, you can use an internally hosted file for more accurate RFI testing.</td>
</tr>
<tr>
<td>Maximum runtime (min)</td>
<td>5</td>
<td>This option manages the amount of time in minutes spent performing web application tests. This option defaults to 60 minutes and applies to all ports and CGIs for a given website. Scanning the local network for web sites with small applications typically completes in under an hour, however web sites with large applications may require a higher value.</td>
</tr>
</tbody>
</table>

### Windows

The Windows section contains the following groups of settings:

- [General Settings](#)
- [User Enumeration Methods](#)
### Request information about the SMB Domain

| Enabled | If enabled, domain users are queried instead of local users. |

### User Enumeration Methods

You can enable as many of the user enumeration methods as appropriate for user discovery.

<table>
<thead>
<tr>
<th>Method</th>
<th>Enabled</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAM Registry</td>
<td>Enabled</td>
<td>Tenable.io enumerates users via the Security Account Manager (SAM) registry.</td>
</tr>
<tr>
<td>ADSI Query</td>
<td>Enabled</td>
<td>Tenable.io enumerates users via Active Directory Service Interfaces (ADSI). To use ADSI, you must configure credentials under <strong>Credentials &gt; Miscellaneous &gt; ADSI</strong>.</td>
</tr>
<tr>
<td>WMI Query</td>
<td>Enabled</td>
<td>Tenable.io enumerates users via Windows Management Interface (WMI).</td>
</tr>
<tr>
<td>RID Brute Forcing</td>
<td>Enabled</td>
<td>Tenable.io enumerates users via relative identifier (RID) brute forcing. Enabling this setting enables the <strong>Enumerate Domain Users</strong> and <strong>Enumerate Local User</strong> settings.</td>
</tr>
</tbody>
</table>

### Enumerate Domain Users (available with RID Brute Forcing enabled)

| Start UID | 1000 | The beginning of a range of IDs where Tenable.io attempts to enumerate domain users. |
| End UID   | 1200 | The end of a range of IDs where Tenable.io attempts to enumerate domain users. |

### Enumerate Local User (available with RID Brute Forcing enabled)

| Start UID | 1000 | The beginning of a range of IDs where Tenable.io attempts to enumerate local users. |
| End UID   | 1200 | The end of a range of IDs where Tenable.io attempts to enumerate local users. |

**Malware**
The **Malware** section contains the following groups of settings:

- **General Settings**
- **Hash and Whitelist Files**
- **Yara Rules**
- **File System Scanning**

### General Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable DNS resolution</td>
<td>Disabled</td>
<td>Checking this option prevents Tenable.io from using the cloud to compare scan findings against known malware.</td>
</tr>
</tbody>
</table>

### Hash and Whitelist Files

<table>
<thead>
<tr>
<th>Custom Netstat IP Threat List</th>
<th>None</th>
<th>A text file that contains a list of known bad IP addresses that you want to detect. Each line in the file must begin with an IPv4 address. Optionally, you can add a description by adding a comma after the IP address, followed by the description. You can also use hash-delimited comments (e.g., #) in addition to comma-delimited comments.</th>
</tr>
</thead>
</table>

**Note:** Tenable does not detect private IP ranges in the text file.

<p>| Provide your own list of known bad MD5 hashes | None | A text file with one MD5 hash per line that specifies additional known bad MD5 hashes. Optionally, you can include a description for a hash by adding a comma after the hash, followed by the description. If any matches are found when scanning a target, the description appears in the scan results. You can also use hash-delimited comments (e.g., #) in |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide your own list of known good MD5 hashes</td>
<td>None</td>
<td>A text file with one MD5 hash per line that specifies additional known good MD5 hashes. Optionally, you can include a description for each hash by adding a comma after the hash, followed by the description. If any matches are found when scanning a target, and a description was provided for the hash, the description appears in the scan results. You can also use hash-delimited comments (e.g., #) in addition to comma-delimited comments.</td>
</tr>
<tr>
<td>Hosts file whitelist</td>
<td>None</td>
<td>Tenable.io checks system hosts files for signs of a compromise (e.g., Plugin ID 23910 titled Compromised Windows System (hosts File Check)). This option allows you to upload a file containing a list of IPs and hostnames you want Tenable.io to ignore during a scan. Include one IP and one hostname (formatted identically to your hosts file on the target) per line in a regular text file.</td>
</tr>
<tr>
<td>Yara Rules</td>
<td>None</td>
<td>A .yar file containing the YARA rules to be applied in the scan. You can only upload one file per scan, so include all rules in a single file. For more information, see <a href="https://yara.readthedocs.io">yara.readthedocs.io</a>.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Scan %Systemroot%</td>
<td>Disabled</td>
<td>Enables file system scanning to scan %Systemroot%.</td>
</tr>
<tr>
<td>Scan %ProgramFiles%</td>
<td>Disabled</td>
<td>Enables file system scanning to scan %ProgramFiles%.</td>
</tr>
<tr>
<td>Scan %ProgramFiles (x86)%</td>
<td>Disabled</td>
<td>Enables file system scanning to scan %ProgramFiles (x86)%.</td>
</tr>
<tr>
<td>Scan %ProgramData%</td>
<td>Disabled</td>
<td>Enables file system scanning to scan %ProgramData%.</td>
</tr>
<tr>
<td>Scan User Profiles</td>
<td>Disabled</td>
<td>Enables file system scanning to scan user profiles.</td>
</tr>
<tr>
<td>Custom Filescan Directories</td>
<td>None</td>
<td>A custom file that lists directories to be scanned by malware file scanning. List each directory on one line.</td>
</tr>
</tbody>
</table>

**Linux Directories**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan $PATH</td>
<td>Disabled</td>
<td>Enables file system scanning to scan $PATH.</td>
</tr>
<tr>
<td>Scan /home</td>
<td>Disabled</td>
<td>Enables file system scanning to scan /home.</td>
</tr>
</tbody>
</table>

**MacOS Directories**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan $PATH</td>
<td>Disabled</td>
<td>Enables file system scanning to scan $PATH.</td>
</tr>
<tr>
<td>Scan /Users</td>
<td>Disabled</td>
<td>Enables file system scanning to scan /Users.</td>
</tr>
<tr>
<td>Scan /Applications</td>
<td>Disabled</td>
<td>Enables file system scanning to scan /Applications.</td>
</tr>
<tr>
<td>Scan /Library</td>
<td>Disabled</td>
<td>Enables file system scanning to scan /Library.</td>
</tr>
</tbody>
</table>

**Databases**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Database</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use detected SIDs</td>
<td>Disabled</td>
<td>When enabled, if at least one <a href="#">host credential</a> and one <a href="#">Oracle database credential</a> are configured, the scanner</td>
</tr>
</tbody>
</table>
| | authenticates to scan targets using the host credentials, and then attempts to detect Oracle System IDs (SIDs) locally. The scanner then attempts to authenticate using the specified Oracle database credentials and the detected SIDs.

If the scanner cannot authenticate to scan targets using host credentials or does not detect any SIDs locally, the scanner authenticates to the Oracle database using the manually specified SIDs in the Oracle database credentials. |
Preconfigured Assessment Settings

Certain Tenable-provided scanner templates include preconfigured assessment settings, described in the following table. The preconfigured assessment settings are determined by both the template and the **Mode** that you select.

<table>
<thead>
<tr>
<th>Template</th>
<th>Mode</th>
<th>Preconfigured Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Scans (Common)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced Network Scan</td>
<td>-</td>
<td><strong>All defaults</strong></td>
</tr>
<tr>
<td>Basic Network Scan</td>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>Scan for known web vulnerabilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• General Settings:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Avoid false alarms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Disable CGI scanning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Web Applications:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Disable web application scanning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• General Settings:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Avoid potential false alarms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Enable CGI scanning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Web Applications:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Start crawling from &quot;/&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Crawl 1000 pages (max)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Traverse 6 directories (max)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Test for known vulnerabilities in commonly used web applications</td>
</tr>
</tbody>
</table>
| Scan for all web vulnerabilities (quick) | • General Settings:  
  ◦ Avoid potential false alarms  
  ◦ Enable CGI scanning  
  • Web Applications:  
  ◦ Start crawling from "/"  
  ◦ Crawl 1000 pages (max)  
  ◦ Traverse 6 directories (max)  
  ◦ Test for known vulnerabilities in commonly used web applications  
  ◦ Perform each generic web app test for 5 minutes (max) |
|---|---|
| Scan for all web vulnerabilities (complex) | • General Settings:  
  ◦ Avoid potential false alarms  
  ◦ Enable CGI scanning  
  ◦ Perform thorough tests  
  • Web Applications:  
  ◦ Start crawling from "/"  
  ◦ Crawl 1000 pages (max)  
  ◦ Traverse 6 directories |
<table>
<thead>
<tr>
<th>Test for known vulnerabilities in commonly used web applications</th>
<th>Test for known vulnerabilities in commonly used web applications</th>
<th>Test for known vulnerabilities in commonly used web applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform each generic web app test for 10 minutes (max)</td>
<td>Perform each generic web app test for 10 minutes (max)</td>
<td>Perform each generic web app test for 10 minutes (max)</td>
</tr>
<tr>
<td>Try all HTTP methods</td>
<td>Try all HTTP methods</td>
<td>Try all HTTP methods</td>
</tr>
<tr>
<td>Attempt HTTP Parameter Pollution</td>
<td>Attempt HTTP Parameter Pollution</td>
<td>Attempt HTTP Parameter Pollution</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Custom</th>
<th>All defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credentialed Patch Audit</td>
<td>All defaults</td>
</tr>
<tr>
<td>Host Discovery</td>
<td>All defaults</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Internal PCI Network Scan</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Applications:</td>
<td>General Settings:</td>
</tr>
<tr>
<td>Disable web application scanning</td>
<td>Avoid false alarms</td>
</tr>
<tr>
<td>Disable CGI scanning</td>
<td>Disable CGI scanning</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scan for known web vulnerabilities</th>
<th>General Settings:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Applications:</td>
<td>Avoid potential false alarms</td>
</tr>
<tr>
<td>Start crawling from &quot;/&quot;</td>
<td>Enable CGI scanning</td>
</tr>
</tbody>
</table>
| Scan for all web vulnerabilities (quick) | • General Settings:  
  - Avoid potential false alarms  
  - Enable CGI scanning  
• Web Applications:  
  - Start crawling from "/"  
  - Crawl 1000 pages (max)  
  - Traverse 6 directories (max)  
  - Test for known vulnerabilities in commonly used web applications  
  - Perform each generic web app test for 5 minutes (max) |
| Scan for all web vulnerabilities (complex) | • General Settings:  
  - Avoid potential false alarms  
  - Enable CGI scanning |
<table>
<thead>
<tr>
<th>Legacy Web App Scan</th>
<th>Custom</th>
<th>All defaults</th>
</tr>
</thead>
</table>
|                      | Scan for known web vulnerabilities | • General Settings:  
  ◦ Avoid potential false alarms  
  ◦ Enable CGI scanning  
  • Web Applications:  
  ◦ Start crawling from "/"  
  ◦ Crawl 1000 pages (max)  
  ◦ Traverse 6 directories (max)  
  ◦ Test for known vulnerabilities in commonly used web applications  
  ◦ Perform each generic web app test for 10 minutes (max)  
  ◦ Try all HTTP methods  
  ◦ Attempt HTTP Parameter Pollution  
  ◦ Perform thorough tests  
  • Web Applications:  
  ◦ Start crawling from "/"  
  ◦ Crawl 1000 pages (max)  
  ◦ Traverse 6 directories (max)  
  ◦ Test for known vulnerabilities in commonly used web applications  
  ◦ Perform each generic web app test for 10 minutes (max)  
  ◦ Try all HTTP methods  
  ◦ Attempt HTTP Parameter Pollution  

Web Applications:

- Start crawling from "/"
- Crawl 1000 pages (max)
- Traverse 6 directories (max)
- Test for known vulnerabilities in commonly used web applications
- Perform each generic web app test for 10 minutes (max)
- Try all HTTP methods
- Attempt HTTP Parameter Pollution

General Settings:

- Avoid potential false alarms
- Enable CGI scanning

Legacy Web App Scan

Scan for known web vulnerabilities
<table>
<thead>
<tr>
<th>Scan for all web vulnerabilities (quick) (Default)</th>
<th>Scan for all web vulnerabilities (complex)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• General Settings:</td>
<td>• General Settings:</td>
</tr>
<tr>
<td>◦ Avoid potential false alarms</td>
<td>◦ Avoid potential false alarms</td>
</tr>
<tr>
<td>◦ Enable CGI scanning</td>
<td>◦ Enable CGI scanning</td>
</tr>
<tr>
<td>• Web Applications:</td>
<td>◦ Perform thorough tests</td>
</tr>
<tr>
<td>◦ Start crawling from &quot;/&quot;</td>
<td>◦ Start crawling from &quot;/&quot;</td>
</tr>
<tr>
<td>◦ Crawl 1000 pages (max)</td>
<td></td>
</tr>
<tr>
<td>◦ Traverse 6 directories (max)</td>
<td></td>
</tr>
<tr>
<td>◦ Test for known vulnerabilities in commonly used web applications</td>
<td>◦ Test for known vulnerabilities in commonly used web applications</td>
</tr>
<tr>
<td>◦ Perform each generic web app test for 5 minutes (max)</td>
<td>◦ Perform each generic web app test for 5 minutes (max)</td>
</tr>
<tr>
<td></td>
<td>Custom</td>
</tr>
<tr>
<td>------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Mobile Device Scan</td>
<td>-</td>
</tr>
<tr>
<td>PCI Quarterly External Scan</td>
<td>-</td>
</tr>
<tr>
<td>Configuration Scans</td>
<td></td>
</tr>
<tr>
<td>Audit Cloud Infrastructure</td>
<td>-</td>
</tr>
<tr>
<td>MDM Config Audit</td>
<td>-</td>
</tr>
<tr>
<td>Offline Config Audit</td>
<td>-</td>
</tr>
<tr>
<td>Policy Compliance Auditing</td>
<td>-</td>
</tr>
<tr>
<td>SCAP and OVAL Auditing</td>
<td>-</td>
</tr>
</tbody>
</table>

- Crawl 1000 pages (max)
- Traverse 6 directories (max)
- Test for known vulnerabilities in commonly used web applications
- Perform each generic web app test for 10 minutes (max)
- Try all HTTP methods
- Attempt HTTP Parameter Pollution
<table>
<thead>
<tr>
<th>Tactical Scans</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Badlock Detection</strong></td>
<td>-</td>
<td><strong>Web Crawler defaults</strong></td>
</tr>
<tr>
<td><strong>Bash Shellshock Detection</strong></td>
<td>-</td>
<td><strong>Web Crawler defaults</strong></td>
</tr>
<tr>
<td><strong>DROWN Detection</strong></td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Intel AMT Security Bypass</strong></td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Malware Scan</strong></td>
<td>-</td>
<td><strong>Malware defaults</strong></td>
</tr>
<tr>
<td><strong>Shadow Brokers Scan</strong></td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Spectre and Meltdown Detection</strong></td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>WannaCry Ransomware Detection</strong></td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Assessment Settings in WAS Scans

Assessment settings specify which web application elements you want the scanner to audit as it crawls your URLs. You can configure Assessment settings when you create a scan or user-defined scan template. For more information, see Scan Templates.

The Assessment settings include the following sections:

- **Scan Type**
- **Elements to Audit**
- **Optional**
- **DOM Element Exclusion**

Scan Type

These settings specify the intensity of the assessment you want the scanner to perform.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment</td>
<td>Recommended</td>
<td>Drop-down box that allows you to choose from the following options to specify the scan type you want the scanner to perform.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Recommended</strong> – The scanner audits elements based on Tenable’s recommendations.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>None</strong> – The scanner does not audit any elements.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Quick</strong> – The scanner audits most the common elements listed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Extensive</strong> – The scanner audits all the elements listed.</td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Custom</td>
<td></td>
<td>Custom – The scanner audits only the elements you select.</td>
<td></td>
</tr>
</tbody>
</table>

### Elements to Audit

These settings specify the elements in your web application that you want the scanner to analyze for vulnerabilities.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Scanner Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cookies</td>
<td>Checks for cookie-based vulnerabilities.</td>
</tr>
<tr>
<td>Headers</td>
<td>Checks for header vulnerabilities and insecure configurations (for example, missing X-Frame-Options).</td>
</tr>
<tr>
<td>Forms</td>
<td>Checks for form-based vulnerabilities.</td>
</tr>
<tr>
<td>Links and Query String Parameters</td>
<td>Checks for vulnerabilities in links and their parameters.</td>
</tr>
<tr>
<td>Parameter Names</td>
<td>Performs extensive fuzzing of parameter names.</td>
</tr>
<tr>
<td>Parameter Values</td>
<td>Performs extensive fuzzing of parameter values.</td>
</tr>
<tr>
<td>Path Parameters</td>
<td>Assesses path parameters. Path parameters are used in URL rewrite to identify the object of the action within the URL. For example, <strong>scanId</strong> is a path parameter for the below URL, used to identify the scan to display results:</td>
</tr>
<tr>
<td></td>
<td><a href="http://example.com/scan/**scanId*/results">http://example.com/scan/**scanId*/results</a></td>
</tr>
<tr>
<td>JSON Elements / Request Body (JSON)</td>
<td>Audits JSON request data.</td>
</tr>
<tr>
<td>XML Elements / Request Body (XML)</td>
<td>Audits XML request data.</td>
</tr>
<tr>
<td>Setting</td>
<td>Scanner Action</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>UI Forms</td>
<td>Checks input and button groups associated with JavaScript code.</td>
</tr>
<tr>
<td>UI Inputs</td>
<td>Checks orphan input elements against associated document object model (DOM) events.</td>
</tr>
</tbody>
</table>

Optional

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL for Remote Inclusion</td>
<td>None</td>
<td>Specifies a file on a remote host that Tenable.io Web Application Scanning can use to test for a Remote File Inclusion (RFI) vulnerability.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the scanner cannot reach the internet, the scanner uses this internally-hosted file for more accurate RFI testing.</td>
</tr>
</tbody>
</table>

**Note:** If you do not specify a file, Tenable.io Web Application Scanning uses a safe, Tenable-hosted file for RFI testing.

DOM Element Exclusion

DOM element exclusions prevent scans from interacting with specific page elements and their children. This setting is available for Scan, Overview, and PCI scan templates.

You can add exclusions by clicking the ✗ button and selecting Text Contents or CSS Attribute.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text Contents</td>
<td>None</td>
<td>Excludes elements based on text contents. For example, if you want to prevent the scanner from clicking a logout button named Log Out, you could match the text Log Out.</td>
</tr>
<tr>
<td>CSS Attribute</td>
<td>None</td>
<td>Excludes elements based on a CSS attribute key-value pair. For example, if you want to prevent the scanner from interacting</td>
</tr>
<tr>
<td>with a form that contains the CSS attribute key-value pair id=&quot;logout&quot;, type id for the key and logout for the value.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Report Settings in Vulnerability Management Scans

**Note:** If a scan is based on a user-defined template, you cannot configure Report settings in the scan. You can only modify these settings in the related user-defined template.

The **Report** settings include the following groups of settings:

- **Processing**
- **Output**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Override normal verbosity</td>
<td>Disabled</td>
<td>When disabled, provides the standard level of plugin activity in the report. The output does not include the informational plugins 56310, 64582, and 58651. When enabled, this setting has two options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>I have limited disk space. Report as little information as possible</strong> — Provides less information about plugin activity in the report to minimize impact on disk space.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Report as much information as possible</strong> — Provides more information about plugin activity in the report. When this option is selected, the output includes the informational plugins 56310, 64582, and 58651.</td>
</tr>
<tr>
<td>Show missing patches that have been superseded</td>
<td>Enabled</td>
<td>When enabled, includes superseded patch information in the scan report.</td>
</tr>
<tr>
<td>Hide results from plugins initiated as a dependency</td>
<td>Enabled</td>
<td>When enabled, the list of dependencies is not included in the report. If you want to include the list of dependencies in the report, disable this setting.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Output</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Designate hosts by their DNS name</td>
<td>Disabled</td>
<td>Uses the host name rather than IP address for report output.</td>
</tr>
<tr>
<td>Display hosts that respond to ping</td>
<td>Disabled</td>
<td>Reports hosts that successfully respond to a ping.</td>
</tr>
<tr>
<td>Display unreachable hosts</td>
<td>Disabled</td>
<td>When enabled, hosts that did not reply to the ping request are included in the security report as dead hosts. Do not enable this option for large IP blocks.</td>
</tr>
<tr>
<td>Display Unicode characters</td>
<td>Disabled</td>
<td>When enabled, Unicode characters appear in plugin output such as usernames, installed application names, and SSL certificate information.</td>
</tr>
</tbody>
</table>

**Note:** Plugin output may sometimes incorrectly parse or truncate strings with Unicode characters. If this issue causes problems with regular expressions in plugins or custom audits, disable this setting and scan again.
Report Settings in WAS Scans

Report settings specify extra items to include in the scan report. For example, scan reports for PCI ASV scans require load balancer usage details if applicable.

You can configure Report settings when you create a scan or user-defined scan template using the Tenable-provided scan template, PCI. For more information, see Scan Templates.

The Report settings include the following sections:

- **(PCI ASV 6.1) Load Balancers Usage**

(PCI ASV 6.1) Load Balancers Usage

This setting specifies load balancer usage to include in the scan report.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>(PCI ASV 6.1) Load Balancers Usage</td>
<td>None</td>
<td>Text box that allows you to enter a list of load balancers and their configuration as required for PCI ASV if applicable.</td>
<td>No</td>
</tr>
</tbody>
</table>

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective
Advanced Settings in Vulnerability Management Scans

Note: If a scan is based on a user-defined template, you cannot configure Advanced settings in the scan. You can only modify these settings in the related user-defined template.

The Advanced settings provide increased control over scan efficiency and the operations of a scan, as well as the ability to enable plugin debugging.

Certain Tenable-provided scanner templates include preconfigured advanced settings.

If you select the Custom preconfigured setting option, or if you are using a scanner template that does not include preconfigured advanced settings, you can manually configure Advanced settings in the following categories:

- General Settings
- Performance Options
- Unix Find Command Exclusions
- Debug Settings
- Stagger Scan Start (Agent scans only)

Note: The following tables include settings for the Advanced Network Scan template. Depending on the template you select, certain settings may not be available, and default values may vary.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Safe Checks</td>
<td>Enabled</td>
<td>When enabled, disables all plugins that may have an adverse effect on the remote host.</td>
</tr>
<tr>
<td>Stop scanning hosts that become unresponsive during the scan</td>
<td>Disabled</td>
<td>When enabled, Tenable.io stops scanning if it detects that the host has become unresponsive. This may occur if users turn off their PCs during a scan, a host has stopped responding after a denial of service plugin, or a security mechanism (for example, an IDS) has started to block traffic to a server. Normally, continuing scans on these hosts makes the scan take longer than necessary, and the results may not be accurate.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Scan IP addresses in a random order</strong></td>
<td>Disabled</td>
<td>By default, Tenable.io scans a list of IP addresses in sequential order. When this option is enabled, Tenable.io scans the list of hosts in a random order within an IP address range. This approach is typically useful in helping to distribute the network traffic during large scans.</td>
</tr>
<tr>
<td><strong>Scan targets with multiple domain names in parallel</strong></td>
<td>Disabled</td>
<td>When disabled, to avoid overwhelming a host, Tenable.io prevents a single scanner from simultaneously scanning multiple targets that resolve to a single IP address. Instead, Tenable.io scanners serialize attempts to scan the IP address, whether it appears more than once in the same scan task or in multiple scan tasks on that scanner. Scans may take longer to complete. When enabled, a Tenable.io scanner can simultaneously scan multiple targets that resolve to a single IP address within a single scan task or across multiple scan tasks. Scans complete more quickly, but hosts could potentially become overwhelmed, causing timeouts and incomplete results.</td>
</tr>
<tr>
<td><strong>Automatically accept detected SSH disclaimer prompts</strong></td>
<td>Disabled</td>
<td>When enabled, if a credentialed scan tries to connect via SSH to a FortiOS host that presents a disclaimer prompt, the scanner provides the necessary text input to accept the disclaimer prompt and continue the scan. When disabled, credentialed scans on hosts that present a disclaimer prompt fail because the scanner cannot connect to the device and accept the disclaimer. The error appears in the plugin output.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Create unique identifier on hosts scanned using credentials</td>
<td>Enabled</td>
<td>When enabled, the scanner creates a unique identifier for credentialed scans.</td>
</tr>
<tr>
<td>Performance Options</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slow down the scan when network congestion is detected</td>
<td>Disabled</td>
<td>When enabled, Tenable.io detects when it is sending too many packets and the network pipe is approaching capacity. If network congestion is detected, Tenable.io throttles the scan to accommodate and alleviate the congestion. Once the congestion has subsided, Tenable.io automatically attempts to use the available space within the network pipe again.</td>
</tr>
<tr>
<td>Use Linux kernel congestion detection</td>
<td>Disabled</td>
<td>When enabled, Tenable.io uses the Linux kernel to detect when it sends too many packets and the network pipe approaches capacity. If detected, Tenable.io throttles the scan to accommodate and alleviate the congestion. Once the congestion subsides, Tenable.io automatically attempts to use the available space within the network pipe again.</td>
</tr>
<tr>
<td>Network timeout (in seconds)</td>
<td>5</td>
<td>Specifies the time that Tenable.io waits for a response from a host unless otherwise specified within a plugin. If you are scanning over a slow connection, you may want to set this to a higher number of seconds.</td>
</tr>
<tr>
<td>Max simultaneous checks per host</td>
<td>5</td>
<td>Specifies the maximum number of checks a Tenable.io scanner will perform against a single host at one time.</td>
</tr>
<tr>
<td>Max simultaneous hosts</td>
<td>depends on the Tenable-</td>
<td>Specifies the maximum number of hosts that a Tenable.io scanner will scan at the same time.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>per scan</td>
<td>provided template used for the scan</td>
<td></td>
</tr>
<tr>
<td>Max number of concurrent TCP sessions per host</td>
<td>none</td>
<td>Specifies the maximum number of established TCP sessions for a single host. This TCP throttling option also controls the number of packets per second the SYN scanner sends, which is 10 times the number of TCP sessions. For example, if this option is set to 15, the SYN scanner sends 150 packets per second at most.</td>
</tr>
<tr>
<td>Max number of concurrent TCP sessions per scan</td>
<td>none</td>
<td>Specifies the maximum number of established TCP sessions for the entire scan, regardless of the number of hosts being scanned. For scanners installed on any Windows host, you must set this value to 19 or less to get accurate results.</td>
</tr>
</tbody>
</table>

**Unix Find Command Exclusions**

<table>
<thead>
<tr>
<th>Custom filepath</th>
<th>none</th>
<th>A plain text file containing a list of filepaths to exclude from all plugins that search using the <code>find</code> command on Unix systems. In the file, enter one filepath per line, formatted per patterns allowed by the Unix <code>find</code> command <code>-path</code> argument. For more information, see the <code>find</code> command man page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom filesystem</td>
<td>none</td>
<td>A plain text file containing a list of filesystems to exclude from all plugins that search using the <code>find</code> command on Unix systems.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>In the file, enter one filesystem per line, using filesystem types supported by the Unix <code>find</code> command <code>-fstype</code> argument. For more information, see the <code>find</code> command man page.</td>
<td>none</td>
<td>A plain text file containing a list of filepaths to include from all plugins that search using the <code>find</code> command on Unix systems.</td>
</tr>
<tr>
<td>Include Filepath</td>
<td>none</td>
<td>In the file, enter one filepath per line, formatted per patterns allowed by the Unix <code>find</code> command <code>-path</code> argument. For more information, see the <code>find</code> command man page.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Including filepaths increases the locations that are searched by plugins, which extends the duration of the scan. Make your inclusions as specific as possible.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Tip:</strong> Avoid having the same filepaths in Include Filepath and Exclude Filepath. This conflict may result in the filepath being excluded from the search, though results may vary by operating system.</td>
</tr>
</tbody>
</table>

**Debug Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable plugin debugging</td>
<td>Disabled</td>
<td>Attaches available debug logs from plugins to the vulnerability output of this scan.</td>
</tr>
<tr>
<td>Audit Trail Verbosity</td>
<td>Default</td>
<td>Controls verbosity of the plugin audit trail.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Options include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>No audit trail</strong> — (Default) Tenable.io does not generate a plugin audit trail.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>All audit trail data</strong> — The audit trail includes the reason why plugins were not included in the scan.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Only scan errors</em> — The audit trail includes only errors encountered during the scan.</td>
</tr>
</tbody>
</table>

**Stagger Scan Start**

| Maximum delay (minutes) | 0              | (Agent scans only) (Agents 8.2 and later) If set, each agent in the agent group delays starting the scan for a random number of minutes, up to the specified maximum. Staggered starts can reduce the impact of agents that use a shared resource, such as virtual machine CPU. If the maximum delay you set exceeds your scan window, Tenable.io shortens your maximum delay to ensure that agents begin scanning at least 30 minutes before the scan window closes. |
Preconfigured Advanced Settings

Certain Tenable-provided scanner templates include preconfigured advanced settings, described in the following table. The preconfigured advanced settings are determined by both the template and the **Mode** that you select.

<table>
<thead>
<tr>
<th>Template</th>
<th>Scan Type</th>
<th>Preconfigured Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Scans (Common)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced Network Scan</td>
<td>-</td>
<td>All defaults</td>
</tr>
<tr>
<td>Basic Network Scan</td>
<td>Default (default)</td>
<td>Performance options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 30 simultaneous hosts (max)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 4 simultaneous checks per host (max)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 5 second network read timeout</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Asset identification options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Create unique identifier on hosts scanned using credentials</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Performance options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 30 simultaneous hosts (max)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 4 simultaneous checks per host (max)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 5 second network read timeout</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Asset identification options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Create unique identifier on hosts scanned using credentials</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Performance options:</td>
</tr>
<tr>
<td>Scan low band-</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| width links                                  | 2 simultaneous hosts (max)  
|                                             | 2 simultaneous checks per host (max)  
|                                             | 15 second network read timeout  
|                                             | Slow down the scan when network congestion is detected  
|                                             | • Asset identification options:  
|                                             | ◦ Create unique identifier on hosts scanned using credentials  
| Custom                                      | All defaults  
| Credentialed Patch Audit                    | Default (default)  
|                                             | • Performance options:  
|                                             | ◦ 30 simultaneous hosts (max)  
|                                             | ◦ 4 simultaneous checks per host (max)  
|                                             | ◦ 5 second network read timeout  
|                                             | • Asset identification options:  
|                                             | ◦ Create unique identifier on hosts scanned using credentials  
| Scan low bandwidth links                     | • Performance options:  
|                                             | ◦ 2 simultaneous hosts (max)  
|                                             | ◦ 2 simultaneous checks per host (max)  
<p>|                                             | ◦ 15 second network read |</p>
<table>
<thead>
<tr>
<th>Host Discovery</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal PCI Network Scan</strong></td>
<td><strong>Default</strong> (default)</td>
<td></td>
</tr>
<tr>
<td><strong>Scan low bandwidth links</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Custom</strong></td>
<td><strong>All defaults</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>timeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ Slow down the scan when network congestion is detected</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Asset identification options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ Create unique identifier on hosts scanned using credentials</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Performance options:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ 30 simultaneous hosts (max)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ 4 simultaneous checks per host (max)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ 5 second network read timeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Asset identification options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ Create unique identifier on hosts scanned using credentials</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Performance options:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ 2 simultaneous hosts (max)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ 2 simultaneous checks per host (max)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ 15 second network read timeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ Slow down the scan when network congestion is detected</td>
<td></td>
</tr>
<tr>
<td>Asset identification options:</td>
<td>Performance options:</td>
<td></td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------</td>
<td></td>
</tr>
<tr>
<td>○ Create unique identifier on hosts scanned using credentials</td>
<td>○ 30 simultaneous hosts (max)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ 4 simultaneous checks per host (max)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ 5 second network read timeout</td>
<td></td>
</tr>
<tr>
<td><strong>Legacy Web App Scan</strong></td>
<td><strong>Default (default)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Asset identification options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Create unique identifier on hosts scanned using credentials</td>
<td></td>
</tr>
<tr>
<td><strong>Scan low bandwidth links</strong></td>
<td></td>
<td>○ Performance options:</td>
</tr>
<tr>
<td></td>
<td>○ 2 simultaneous hosts (max)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ 2 simultaneous checks per host (max)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ 15 second network read timeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Slow down the scan when network congestion is detected</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Asset identification options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Create unique identifier on hosts scanned using credentials</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Custom</td>
<td>All defaults</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Mobile Device Scan</td>
<td>-</td>
<td>Debug Settings defaults</td>
</tr>
<tr>
<td>PCI Quarterly External Scan</td>
<td>Default (default)</td>
<td>• Performance options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ 20 simultaneous hosts (max)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ 4 simultaneous checks per host (max)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ 15 second network read timeout</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Slow down the scan when network congestion is detected</td>
</tr>
<tr>
<td>Scan low bandwidth links</td>
<td></td>
<td>• Performance options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ 2 simultaneous hosts (max)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ 2 simultaneous checks per host (max)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ 15 second network read timeout</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Slow down the scan when network congestion is detected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Asset identification options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Create unique identifier on hosts scanned using credentials</td>
</tr>
<tr>
<td>Custom</td>
<td></td>
<td>• Performance Options (default options)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unix Find Command Exclusions (default options)</td>
</tr>
<tr>
<td>Configuration Scans</td>
<td>Debug Settings defaults</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------</td>
<td></td>
</tr>
<tr>
<td>Audit Cloud Infrastructure</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>MDM Config Audit</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Offline Config Audit</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Policy Compliance Auditing</td>
<td>Default (default)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Performance options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ 30 simultaneous hosts (max)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ 4 simultaneous checks per host (max)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ 5 second network read timeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Asset identification options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Create unique identifier on hosts scanned using credentials</td>
<td></td>
</tr>
<tr>
<td>Scan low bandwidth links</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Performance options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ 2 simultaneous hosts (max)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ 2 simultaneous checks per host (max)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ 15 second network read timeout</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Slow down the scan when network congestion is detected</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Asset identification options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>○ Create unique identifier on hosts scanned using credentials</td>
<td></td>
</tr>
<tr>
<td>Custom</td>
<td>All defaults</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td><strong>SCAP and OVAL Auditing</strong></td>
<td><strong>Default</strong> (default)</td>
<td></td>
</tr>
<tr>
<td>Performance options:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 30 simultaneous hosts (max)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 4 simultaneous checks per host (max)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 5 second network read timeout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset identification options:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Create unique identifier on hosts scanned using credentials</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Scan low bandwidth links</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance options:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 2 simultaneous hosts (max)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 2 simultaneous checks per host (max)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 15 second network read timeout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Slow down the scan when network congestion is detected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset identification options:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Create unique identifier on hosts scanned using credentials</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Tactical Scans</strong></td>
<td><strong>All defaults</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Badlock Detection</strong></td>
<td><strong>All defaults</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Bash Shellshock Detection</strong></td>
<td><strong>All defaults</strong></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>DROWN Detection</strong></td>
<td>-</td>
<td><strong>All defaults</strong></td>
</tr>
<tr>
<td><strong>Intel AMT Security Bypass</strong></td>
<td>-</td>
<td><strong>All defaults</strong></td>
</tr>
<tr>
<td><strong>Malware Scan</strong></td>
<td><strong>Default</strong> (default)</td>
<td>• Performance options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ 30 simultaneous hosts (max)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ 4 simultaneous checks per host (max)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ 5 second network read timeout</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Asset identification options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Create unique identifier on hosts scanned using credentials</td>
</tr>
<tr>
<td><strong>Scan low bandwidth links</strong></td>
<td></td>
<td>• Performance options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ 2 simultaneous hosts (max)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ 2 simultaneous checks per host (max)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ 15 second network read timeout</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Slow down the scan when network congestion is detected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Asset identification options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Create unique identifier on hosts scanned using credentials</td>
</tr>
<tr>
<td><strong>Custom</strong></td>
<td></td>
<td><strong>All defaults</strong></td>
</tr>
<tr>
<td>Shadow Brokers Scan</td>
<td>-</td>
<td>All defaults</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Spectre and Meltdown Detection</td>
<td>-</td>
<td>All defaults</td>
</tr>
<tr>
<td>WannaCry Ransomware Detection</td>
<td>-</td>
<td>All defaults</td>
</tr>
</tbody>
</table>
Advanced Settings in WAS Scans

Advanced settings specify additional controls you want to implement in a web application scan.

You can configure Advanced settings when you create a scan or user-defined scan template using any Tenable-provided scan template. However, the Overview and Scan template types have more configurable Advanced settings than the Config Audit and SSL TLS template types. For more information, see Scan Templates.

The Advanced Settings options allow you to control the efficiency and performance of the scan.

- **General**
- **HTTP Settings**
- **Screen Settings**
- **Limits**
- **Selenium Settings**
- **Performance Settings**

**General**

You can configure General options in scans and user-defined scan templates based on the Overview and Scan templates only.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Scan Max Time (HH:MM:SS)</td>
<td>08:00:00</td>
<td>Specifies the maximum duration the scanner runs a scan job runs before stopping, displayed in hours, minutes, and seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: The maximum duration you can set for your overall scan max time is 99:59:59 (hours: minutes: seconds).</td>
</tr>
<tr>
<td>Enable Debug logging for this scan</td>
<td>disabled</td>
<td>Specifies whether the scanner attaches available debug logs from plugins to the vulnerability output of this scan.</td>
</tr>
</tbody>
</table>
HTTP Settings

These settings specify the user-agent you want the scanner to identify and the HTTP response headers you want the scanner to include in requests to the web application.

You can configure **Crawl Settings** options in scans and user-defined scan templates based on any Tenable-provided scan template.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a different User Agent to identify scanner</td>
<td>disabled</td>
<td>Specifies whether you want the scanner to use a user-agent header other than Chrome when sending an HTTP request.</td>
</tr>
<tr>
<td>User Agent</td>
<td>Chrome's user-agent</td>
<td>Specifies the name of the user-agent header you want the scanner to use when sending an HTTP request. By default, Tenable.io Web Application Scanning uses the user-agent that Chrome uses for the operating system and platform that corresponds to your machine's operating system and platform. For more information about Chrome's user-agents, see the <em>Google Chrome Documentation</em>. You can configure this option only after you select the <strong>Use a different User Agent to identify scanner</strong> check box.</td>
</tr>
<tr>
<td>Add Scan ID HTTP Header</td>
<td>disabled</td>
<td>Specifies whether the scanner adds an additional X-Tenable-Was-Scan-Id header (set with the scan ID) to all HTTP requests sent to the target, which allows you to easily identify scan jobs in web server logs and modify your scan configurations to better secure your sites.</td>
</tr>
<tr>
<td>Custom Headers</td>
<td>none</td>
<td>Specifies the custom headers you want to inject into each HTTP request, in request and response format. You can add additional custom headers by clicking the + button and typing the values for each additional header.</td>
</tr>
</tbody>
</table>
Note: If you enter a custom User-Agent header, that value will override the value entered in the User Agent setting box.

Screen Settings

You can configure Screen Settings options in scans and user-defined scan templates based on the Overview and Scan templates only.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screen Width</td>
<td>1600</td>
<td>Specifies the screen width, in pixels, of the browser embedded in the scanner.</td>
</tr>
<tr>
<td>Screen Height</td>
<td>1200</td>
<td>Specifies the screen height, in pixels, of the browser embedded in the scanner.</td>
</tr>
<tr>
<td>Ignore Images</td>
<td>disabled</td>
<td>Specifies if the browser embedded in the scanner crawls or ignores images on your target web pages.</td>
</tr>
</tbody>
</table>

Limits

You can configure Limits options in scans and user-defined scan templates based on the Overview and Scan templates only.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of URLs to Crawl and Browse</td>
<td>10000</td>
<td>Specifies the maximum number of URLs the scanner attempts to crawl.</td>
</tr>
<tr>
<td>Path Directory Depth</td>
<td>10</td>
<td>Specifies the maximum number of sub-directories the scanner crawls.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, if your target is <a href="http://www.example.com">www.example.com</a>, and you want the scanner to crawl <a href="http://www.example.com/users/mynname">www.example.com/users/mynname</a>, type 2 in the text box.</td>
</tr>
<tr>
<td>Page DOM Element</td>
<td>5</td>
<td>Specifies the maximum number of HTML nested ele-</td>
</tr>
</tbody>
</table>

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable,Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective
ment Depth | \(500000\) | Specifies the maximum load size of a page, in bytes, the scanner analyzes. If the scanner crawls a URL and the response exceeds the limit, the scanner does not analyze the page for vulnerabilities.

Selenium Settings

These settings specify how the scanner behaves when it attempts to authenticate to a web application using your recorded Selenium credentials.

Configure these options if you configured your scan to authenticate to the web application with Selenium credentials. For more information see [Credentials in WAS Scans](#).

You can configure **Selenium Settings** options in scans and user-defined scan templates based on the **Overview** and **Scan** templates only.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page Rendering Delay</td>
<td>30000</td>
<td>Specifies the time, in milliseconds, the scanner waits for the page to render.</td>
</tr>
<tr>
<td>Command Execution Delay</td>
<td>500</td>
<td>Specifies the time, in milliseconds, the scanner waits after processing a command before proceeding to the next command.</td>
</tr>
<tr>
<td>Script Completion Delay</td>
<td>5000</td>
<td>Specifies the time, in milliseconds, the scanner waits for all commands to render new content to finish processing.</td>
</tr>
</tbody>
</table>

Performance Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Number of Con-</td>
<td>10</td>
<td>Specifies the maximum number of established</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>current HTTP Connections</td>
<td></td>
<td>HTTP sessions allowed for a single host.</td>
</tr>
<tr>
<td>Max Number of HTTP Requests Per Second</td>
<td>25</td>
<td>Specifies the maximum number of HTTP requests allowed for a single host for the duration of the scan.</td>
</tr>
<tr>
<td>Slow down the scan when network congestion is detected</td>
<td>disabled</td>
<td>Specifies whether the scanner throttles the scan in the event of network congestion.</td>
</tr>
<tr>
<td>Network Timeout (In Seconds)</td>
<td>5</td>
<td>Specifies the time, in seconds, the scanner waits for a response from a host before aborting the scan, unless otherwise specified in a plugin. If your internet connection is slow, Tenable recommends that you specify a longer wait time.</td>
</tr>
<tr>
<td>Browser Timeout (In Seconds)</td>
<td>30</td>
<td>Specifies the time, in seconds, the scanner waits for a response from a browser before aborting the scan, unless otherwise specified in a plugin. If your internet connection is slow, Tenable recommends that you specify a longer wait time.</td>
</tr>
<tr>
<td>Timeout Threshold</td>
<td>100</td>
<td>Specifies the number of consecutive timeouts allowed before the scanner aborts the scan.</td>
</tr>
</tbody>
</table>
Credentials in Vulnerability Management Scans

You can use credentials to grant a Tenable.io scanner local access to scan a target system without requiring an agent. Credentialed scans can perform a wider variety of checks than non-credentialed scans, which can result in more accurate scan results. This approach facilitates scanning of a very large network to determine local exposures or compliance violations.

Credentialed scans can perform any operation that a local user can perform. The level of scanning depends on the privileges granted to the user account. The more privileges the scanner has via the login account (for example, root or administrator access), the more thorough the scan results.

In Tenable.io, you can create credentials for use in scans in the following ways:

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan-specific</td>
<td>• You configure and store these credentials in an individual scan.</td>
<td>User Permissions in Basic settings in the scan</td>
</tr>
<tr>
<td></td>
<td>• If you delete the scan, you also delete the credentials.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If you want to use the credentials in a different scan, you must either convert the scan-specific credential to a managed credential or recreate the scan-specific credential settings in the other scan.</td>
<td></td>
</tr>
<tr>
<td>Template-specific</td>
<td>• You configure and store these credentials in a user-defined template. You can then use the template to create individual scans.</td>
<td>User Permissions in Basic settings in the template</td>
</tr>
<tr>
<td></td>
<td>• If you add credentials to a user-defined template, other users can override those credentials by adding scan-specific or managed credentials to scans created from the template. Tenable recommends adding managed credentials to scans, instead of adding credentials to user-defined templates.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If you delete the template, you also delete the template.</td>
<td></td>
</tr>
</tbody>
</table>
plate-specific credentials. However, Tenable.io retains the credentials in any scans you used the template to create before deletion.

- If you want to use the credentials in a different template, you must recreate the template-specific credentials in the other template.

<table>
<thead>
<tr>
<th>Managed</th>
<th>Tenable.io stores managed credentials centrally in the credential manager. You can configure managed credentials directly in the credential manager or during scan configuration. You can also convert a scan-specific credential to a managed credential during scan configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>You can use managed credentials in multiple scans. You can also grant other users permissions to use managed credentials in scans.</td>
</tr>
<tr>
<td></td>
<td>You cannot use managed credentials in templates.</td>
</tr>
</tbody>
</table>

The settings you configure for a credential vary based on the credential type. Credential types include:

- **Cloud Services**
- **Database**
- **Host**
- **Miscellaneous**
- **Mobile Device Management**
- **Patch Management**
- **Plaintext authentication**

For more information, see:
• Add a Credential to a Scan

• Edit a Credential in a Scan

• Convert a Scan-specific Credential to a Managed Credential

• Add a Credential to a User-defined Template

• Edit a Credential in a User-defined Template

**Note:** Tenable.io opens several concurrent authenticated connections. Ensure that the host being audited does not have a strict account lockout policy based on concurrent sessions.

**Note:** By default, when creating credentialed scans or user-defined templates, hosts are identified and marked with a **Tenable Asset Identifier (TAI)**. This globally unique identifier is written to the host's registry or file system, and subsequent scans can retrieve and use the **TAI**.

This option is enabled (by default) or disabled in the **Advanced -> General Settings** of a scan configuration or template: **Create unique identifier on hosts scanned using credentials.**
Add a Credential to a Scan

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can Control

In the event that a scan contains multiple instances of a single type of credential (SSH logins, SMB logins, etc.), Tenable.io attempts to use them on a valid target in the order that they were added to the scan configuration.

**Note:** The first credential that allows successful login is used to perform credentialed checks on the target. After a credential provides successful login, Tenable.io does not try any of the other credentials in the list, even if one of the later credentials has a greater degree of access or privileges.

To add a credential to a scan:

1. Create or edit a scan.

2. In the left navigation menu, click **Credentials**.

   The **Credentials** page appears. This page contains a table of credentials configured for the scan.

3. Next to **Add Credentials**, click the **+** button.

   The **Select Credential Type** plane appears.

4. Do one of the following:

   **Add an existing managed credential.**

   The **Managed Credentials** section of the **Select Credential Type** plane contains any credentials where you have **Can Use** or **Can Edit** permissions.

   a. (Optional) Search for a managed credential in the list by typing your search criteria in the text box and clicking the **🔍** button.
b. In the **Managed Credentials** section, click the \( \bigvee \) button to display all managed credentials.

c. Click each managed credential you want to add.

   The **Select Credential Type** plane remains open.

d. To close the **Select Credential Type** plane, click the \( \times \) button in the upper-right corner of the plane.

### Add a scan-specific credential.

a. In the **Select Credential Type** plane, in any section except **Managed Credentials**, click the \( \bigvee \) button to display the credentials for that type.

b. Click each credential you want to add.

   The settings plane for that credential type appears.

c. Configure the **settings** for the individual credential configuration.

### Add a new managed credential.

a. In any section of the **Select Credential Type** plane except the **Managed Credentials** section, click the \( \bigvee \) button to display the credentials for that type.

b. Click each credential you want to add.

   The settings plane for that credential type appears.

c. Configure the **settings** for the new managed credential.

d. Click the **Save to Managed Credentials** toggle.

   The managed credential settings appear.

e. In the first text box, type a name for the managed credential.

f. (Optional) In the second text box, type a brief description of the managed credential.

g. **Configure** user permissions for the managed credential.
5. Click **Save** to save your credential changes.

   Tenable.io closes the settings plane and adds the credential to the credentials table for the scan.

6. Do one of the following:

   - If you want to save without launching the scan, click **Save**.
     
     Tenable.io saves the scan.

   - If you want to save and launch the scan immediately, click **Save & Launch**.

     **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

     Tenable.io saves and launches the scan.
Edit a Credential in a Scan

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can Configure

To edit a credential in a scan:

1. **Edit** a scan.

2. In the left navigation menu, click **Credentials**.
   
   A table of credentials configured for the scan appears.

3. In the credentials table, click the credential you want to edit.
   
   The credential settings plane appears.

4. Do one of the following:
   
   - For scan-specific credentials, configure the **settings** for the credential.
   
   - For managed credentials:
     
     a. Edit the name or description.
     
     b. **Configure** the credential settings.
     
     c. **Configure** user permissions for the managed credential.

   * **Note:** You can only view or edit settings for managed credentials where you have **Can Edit** permissions.

5. Click **Save** to save your changes to the credential.
   
   If you edited a managed credential, Tenable.io determines whether any other scans use the managed credential and prompts you to confirm the changes.

6. (Managed credentials only) Click **Yes** to save the changes to the managed credential.

7. Click **Save** to save your scan changes.
Convert a Scan-specific Credential to a Managed Credential

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Owner

A scan-specific credential can only be used in a single scan. To reuse a scan-specific credential in multiple scans, convert it to a managed credential.

To convert a scan-specific credential:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, in the **Vulnerability Management** section, click **Scans**.
   
   The **Scans** page appears.

3. For Vulnerability Management scans, in the **Folders** section, click a folder to load the scans you want to view.
   
   The scans table updates to display the scans in the folder you selected.

4. In the scans table, click the scan you want to edit.
   
   The **Scan Details** page appears.

5. Next to the scan name, click the button.
   
   The **Update a Scan** page appears.

6. In the left navigation menu, click **Credentials**.
   
   A table of credentials configured for the scan appears.

7. In the credentials table, click the scan-specific credential you want to convert.
   
   The credential settings plane appears.
8. Click the **Save to Managed Credentials** toggle.

   The managed credential settings appear.

9. In the first text box, type a name for the managed credential.

10. (Optional) In the second text box, type a brief description of the managed credential.

11. **Configure** user permissions for the managed credential.

12. Click **Save** to save your credential changes.

   Tenable.io closes the settings plane and adds the credential to the credentials table for the scan.

13. Click **Save** to save your scan changes.

   Tenable.io
Add a Credential to a User-defined Template

Required Tenable.io Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Template Permissions: Can Configure

Before you add credentials to a user-defined template, consider the following:

- Other users can override template-specific credentials by adding scan-specific or managed credentials to scans created from the template. Tenable recommends adding managed credentials to scans, instead of adding credentials to user-defined templates.

- You cannot use managed credentials in user-defined templates. To use a single set of credentials for multiple scans, add managed credentials to scans, instead of adding credentials to user-defined templates.

Note: In scan configurations, the Scan-wide Credential Type settings are located in individual credentials. In user-defined templates, these settings are located in the Authentication section of the Basic settings for the template.

To add a template-specific credential:

1. Create or edit a template.

2. In the left navigation menu, click Credentials.

   The Credentials page appears. This page contains a table of credentials configured for the template.

3. Next to Add Credentials, click the button.

   The Select Credential Type plane appears.

4. In the Select Credential Type plane, click a credential type.

   The settings plane for that credential type appears.

5. Configure the settings for the individual credential configuration.
6. Click **Save** to save your credential changes.

   Tenable.io closes the settings plane and adds the credential to the credentials table for the template.

7. Click **Save** to save your template changes.

   Tenable.io adds the credential to the credentials table for the template.
Edit a Credential in a User-defined Template

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Template Permissions:** Can Configure

To edit a credential in a user-defined template:

1. **Edit** a user-defined template.
2. In the left navigation menu, click **Credentials**.
   - A table of credentials configured for the template appears.
3. In the credentials table, click the credential you want to edit.
   - The credential settings plane appears.
4. Configure the **settings** for the credential.
5. Click **Save** to save your changes to the credential.
6. Click **Save** to save your changes to the template.
Cloud Services

Tenable.io can authenticate a scan using accounts in the cloud services listed below.

AWS

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Access Key IDS</td>
<td>-</td>
<td>The AWS access key ID string.</td>
<td>yes</td>
</tr>
<tr>
<td>AWS Secret Key</td>
<td>-</td>
<td>AWS secret key that provides the authentication for AWS Access Key ID.</td>
<td>yes</td>
</tr>
</tbody>
</table>

Scan-wide Credential Type Settings

| Regions to access | Rest of the World | In order for Tenable.io to audit an Amazon AWS account, you must define the regions you want to scan. Per Amazon policy, you need different credentials to audit account configuration for the China region than you do for the rest of the world. Possible regions include: |
|-------------------|-------------------|-----------------------------------------------------------------------------|----------|
|                   |                   | • **GovCloud** – If you select this region, you automatically select the government cloud (e.g., us-gov-west-1). |
|                   |                   | • **Rest of the World** – If you select this region, the following additional options appear: |
|                   |                   | • us-east-1                                                                |          |
|                   |                   | • us-east-2                                                                |          |
|                   |                   | • us-west-1                                                                |          |
|                   |                   | • us-west-2                                                                |          |
- **China** – If you select this region, the following additional options appear:
  - cn-north-1
  - cn-northwest-1

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>Enabled</td>
<td>Whether Tenable.io authenticates over an encrypted (HTTPS) or an unencrypted (HTTP) connection.</td>
<td>no</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>Enabled</td>
<td>Whether Tenable.io verifies the validity of the SSL digital certificate.</td>
<td>no</td>
</tr>
</tbody>
</table>

### Microsoft Azure

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>-</td>
<td>Username required to log in to Microsoft Azure.</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>-</td>
<td>Password associated with the username.</td>
<td>yes</td>
</tr>
<tr>
<td>Client Id</td>
<td>-</td>
<td>The application ID (also known as client ID)</td>
<td>yes</td>
</tr>
</tbody>
</table>
ID) for your registered application.

**Scan-wide Credential Type Settings**

| Subscription IDs | - | List subscription IDs to scan, separated by a comma. If this field is blank, all subscriptions are audited. | no |

**Office 365**

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>-</td>
<td>Username required to log in to Office 365.</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>-</td>
<td>Password associated with the username.</td>
<td>yes</td>
</tr>
<tr>
<td>Client ID</td>
<td>-</td>
<td>The application ID (also known as client ID) for your registered application.</td>
<td>yes</td>
</tr>
<tr>
<td>Client Secret</td>
<td>-</td>
<td>The secret key for your registered application.</td>
<td>yes</td>
</tr>
</tbody>
</table>

**Rackspace**

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>-</td>
<td>Username to log in.</td>
<td>yes</td>
</tr>
<tr>
<td>Password or API Key</td>
<td>-</td>
<td>Password or API key associated with the username.</td>
<td>yes</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>API-Key</td>
<td>Select <strong>Password</strong> or <strong>API-Key</strong> from the drop-down box.</td>
<td>yes</td>
</tr>
<tr>
<td>Scan-wide Credential Type Settings</td>
<td>all locations selected</td>
<td>Location of the Rackspace Cloud instance. Possible locations include:</td>
<td>no</td>
</tr>
</tbody>
</table>
- Dallas-Fort Worth (DFW)
- Chicago (ORD)
- Northern Virginia (IAD)
- London (LON)
- Syndney (SYD)
- Hong Kong (HKG)

### Salesforce.com

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>-</td>
<td>Username required to log in to Salesforce.com</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>-</td>
<td>Password associated with the Salesforce.com username</td>
<td>yes</td>
</tr>
</tbody>
</table>
Database Credentials

The following are available Database credentials:

- **DB2**
- **MySQL**
- **Oracle**
- **PostgreSQL**
- **SQL Server**
- **Sybase ASE**
- **MongoDB**
- **Cassandra**

**DB2**

The following table describes the additional options to configure for DB2 credentials.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auth Type</strong></td>
<td>The authentication method for providing the required credentials.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Password</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Import</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>CyberArk</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Lieberman</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Hashicorp Vault</strong></td>
</tr>
<tr>
<td></td>
<td>For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.</td>
</tr>
<tr>
<td><strong>Database Port</strong></td>
<td>The TCP port that the IBM DB2 database instance listens on for communications from Tenable.io. The default is port 50000.</td>
</tr>
<tr>
<td>Options</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Database Name</td>
<td>The name for your database (not the name of your instance).</td>
</tr>
</tbody>
</table>

**MySQL**

The following table describes the additional options to configure for MySQL credentials.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Type</td>
<td>The authentication method for providing the required credentials.</td>
</tr>
<tr>
<td></td>
<td>• Password</td>
</tr>
<tr>
<td></td>
<td>• Import</td>
</tr>
<tr>
<td></td>
<td>• CyberArk</td>
</tr>
<tr>
<td></td>
<td>• Lieberman</td>
</tr>
<tr>
<td></td>
<td>• Hashicorp Vault</td>
</tr>
</tbody>
</table>

For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username for a user on the database.</td>
</tr>
<tr>
<td>Password</td>
<td>The password associated with the username you provided.</td>
</tr>
<tr>
<td>Database Port</td>
<td>The TCP port that the MySQL database instance listens on for communications from Tenable.io. The default is port 3306.</td>
</tr>
</tbody>
</table>

**Oracle**

The following table describes the additional options to configure for Oracle credentials.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Type</td>
<td>The authentication method for providing the required credentials.</td>
</tr>
<tr>
<td></td>
<td>• Password</td>
</tr>
</tbody>
</table>
For descriptions of the options for your selected authentication type, see [Database Credentials Authentication Types](#).

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Port</td>
<td>The TCP port that the Oracle database instance listens on for communications from Tenable.io. The default is port 1521.</td>
</tr>
<tr>
<td>Auth Type</td>
<td>The type of account you want Tenable.io to use to access the database instance:</td>
</tr>
<tr>
<td></td>
<td>• <strong>SYSDBA</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>SYSOPER</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>NORMAL</strong></td>
</tr>
<tr>
<td>Service Type</td>
<td>The Oracle parameter you want to use to specify the database instance: <strong>SID</strong> or <strong>SERVICE_NAME</strong>.</td>
</tr>
<tr>
<td>Service</td>
<td>The <strong>SID</strong> value or <strong>SERVICE_NAME</strong> value for your database instance. The <strong>Service</strong> value you enter must match your parameter selection for the <strong>Service Type</strong> option.</td>
</tr>
</tbody>
</table>

**PostgreSQL**

The following table describes the additional options to configure for **PostgreSQL** credentials.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Type</td>
<td>The authentication method for providing the required credentials.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Password</strong></td>
</tr>
</tbody>
</table>
### Options

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Port</td>
<td>The TCP port that the PostgreSQL database instance listens on for communications from Tenable.io. The default is port 5432.</td>
</tr>
<tr>
<td>Database Name</td>
<td>The name for your database instance.</td>
</tr>
</tbody>
</table>

### SQL Server

The following table describes the additional options to configure for **SQL Server** credentials.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Type</td>
<td>The authentication method for providing the required credentials.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Password</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Import</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>CyberArk</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Lieberman</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Hashicorp Vault</strong></td>
</tr>
<tr>
<td></td>
<td>For descriptions of the options for your selected authentication type, see <strong>Database Credentials Authentication Types</strong>.</td>
</tr>
<tr>
<td>Username</td>
<td>The username for a user on the database.</td>
</tr>
<tr>
<td>Password</td>
<td>The password associated with the username you provided.</td>
</tr>
<tr>
<td>Options</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Database Port</td>
<td>The TCP port that the SQL Server database instance listens on for communications from Tenable.io. The default is port 1433.</td>
</tr>
<tr>
<td>AuthType</td>
<td>The type of account you want Tenable.io to use to access the database instance: <strong>SQL</strong> or <strong>Windows</strong>.</td>
</tr>
<tr>
<td>Instance Name</td>
<td>The name for your database instance.</td>
</tr>
</tbody>
</table>

**Sybase ASE**

The following table describes the additional options to configure for **Sybase ASE** credentials.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Type</td>
<td>The authentication method for providing the required credentials.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Password</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>CyberArk</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Lieberman</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>Hashicorp Vault</strong></td>
</tr>
<tr>
<td>Database Port</td>
<td>The TCP port that the Sybase ASE database instance listens on for communications from Tenable.io. The default is port 3638.</td>
</tr>
<tr>
<td>Auth Type</td>
<td>The type of authentication used by the Sybase ASE database: <strong>RSA</strong> or <strong>Plain Text</strong>.</td>
</tr>
</tbody>
</table>

**Cassandra**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Type</td>
<td>The authentication method for providing the required credentials.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td><strong>Password</strong></td>
</tr>
<tr>
<td></td>
<td><strong>CyberArk</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Lieberman</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Hashicorp Vault</strong></td>
</tr>
</tbody>
</table>

For descriptions of the options for your selected authentication type, see [Database Credentials Authentication Types](#).

| Port | The port the database listens on. The default is port 9042. |

**MongoDB**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>(Required) The username for the database.</td>
</tr>
<tr>
<td>Password</td>
<td>(Required) The password for the supplied username.</td>
</tr>
<tr>
<td>Database</td>
<td>The name of the database to audit.</td>
</tr>
<tr>
<td>Port</td>
<td>(Required) The TCP port that the MongoDB database instance listens on for communications from Tenable.io.</td>
</tr>
</tbody>
</table>
Database Credentials Authentication Types

Depending on the authentication type you select for your Database credentials, you must configure the following options.

- **Client Certificate**
- **Password**
- **Import**
- **CyberArk (Legacy)**
- **HashiCorp Vault**
- **Lieberman**

Client Certificate

The Client Certificate authentication type is supported for PostgreSQL databases only.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username for the database.</td>
<td>yes</td>
</tr>
<tr>
<td>Client Certificate</td>
<td>The file that contains the PEM certificate for the database.</td>
<td>yes</td>
</tr>
<tr>
<td>Client CA Certificate</td>
<td>The file that contains the PEM certificate for the database.</td>
<td>yes</td>
</tr>
<tr>
<td>Client Certificate Private Key</td>
<td>The file that contains the PEM private key for the client certificate.</td>
<td>yes</td>
</tr>
<tr>
<td>Client Certificate Private Key Passphrase</td>
<td>The passphrase for the private key, if required in your authentication implementation.</td>
<td>no</td>
</tr>
<tr>
<td>Database Port</td>
<td>The port on which Tenable.io communicates with the database.</td>
<td>yes</td>
</tr>
<tr>
<td>Database Name</td>
<td>The name of the database.</td>
<td>no</td>
</tr>
</tbody>
</table>
### Password

<table>
<thead>
<tr>
<th>Option</th>
<th>Database Types</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>All</td>
<td>The username for a user on the database.</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>All</td>
<td>The password for the supplied username.</td>
<td>no</td>
</tr>
<tr>
<td>Database Port</td>
<td>All</td>
<td>The port on which Tenable.io communicates with the database.</td>
<td>yes</td>
</tr>
<tr>
<td>Database Name</td>
<td>DB2, PostgreSQL</td>
<td>The name of the database.</td>
<td>no</td>
</tr>
</tbody>
</table>
| Auth type       | Oracle, SQL Server, Sybase ASE | SQL Server values include:        
|                 |                | • Windows                      
|                 |                | • SQL                          
|                 |                | Oracle values include:          
|                 |                | • SYSDBA                       
|                 |                | • SYSOPER                      
|                 |                | • NORMAL                       
|                 |                | Sybase ASE values include:      
|                 |                | • RSA                          
|                 |                | • Plain Text                   
| Instance name   | SQL Server     | The name for your database instance.                                       | no       |
## Option

<table>
<thead>
<tr>
<th>Option</th>
<th>Database Types</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service type</td>
<td>Oracle</td>
<td>Valid values include:</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SID</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SERVICE_NAME</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Oracle</td>
<td>The SID value for your database instance or a SERVICE_NAME</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td></td>
<td>value. The Service value you enter must match your parameter</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>selection for the Service Type option.</td>
<td></td>
</tr>
</tbody>
</table>

### Import

Upload a `.csv` file with the credentials entered in the specified format. For descriptions of valid values to use for each item, see [Database Credentials](#).

You must configure either CyberArk or HashiCorp credentials for a database credential in the same scan so that Tenable.io can retrieve the credentials.

### Database Credential CSV Format

<table>
<thead>
<tr>
<th>Database Credential</th>
<th>CSV Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2</td>
<td>target, port, database_name, username, cred_manager, accountname_or_secretname</td>
</tr>
<tr>
<td>MySQL</td>
<td>target, port, database_name, username, cred_manager, accountname_or_secretname</td>
</tr>
<tr>
<td>Oracle</td>
<td>target, port, service_type, service_ID, username, auth_type, cred_manager, accountname_or_secretname</td>
</tr>
<tr>
<td>SQL Server</td>
<td>target, port, instance_name, username, auth_type, cred_manager, accountname_or_secretname</td>
</tr>
</tbody>
</table>
**Note:** Include the required data in the specified order, with commas between each value, without spaces. For example, for Oracle with CyberArk: `192.0.2.255,1521,SID,service_id,username,SYSDBA,CyberArk,Database-Oracle-SYS.

**Note:** The value for cred_manager must be either CyberArk or HashiCorp.

## CyberArk

CyberArk is a popular enterprise password vault that helps you manage privileged credentials. Tenable.io can get credentials from CyberArk to use in a scan.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>CyberArk Host</td>
<td>The IP address or FQDN name for the CyberArk AIM Web Service.</td>
<td>yes</td>
</tr>
<tr>
<td>Port</td>
<td>The port on which the CyberArk API communicates. By default, Tenable.io uses 443.</td>
<td>no</td>
</tr>
<tr>
<td>AppID</td>
<td>The Application ID associated with the CyberArk API connection.</td>
<td>yes</td>
</tr>
<tr>
<td>Client Certificate</td>
<td>The file that contains the PEM certificate used to communicate with the CyberArk host.</td>
<td>no</td>
</tr>
<tr>
<td>Client Certificate Private Key</td>
<td>The file that contains the PEM private key for the client certificate.</td>
<td>no</td>
</tr>
<tr>
<td>Client Certificate Private Key Passphrase</td>
<td>The passphrase for the private key, if required.</td>
<td>yes, if private key requires</td>
</tr>
<tr>
<td>Get credential by</td>
<td>The method with which your CyberArk API credentials are retrieved: <strong>Username</strong> or <strong>Identifier</strong></td>
<td>yes</td>
</tr>
<tr>
<td>Username</td>
<td>(If <strong>Get credential by</strong> is set to <strong>Username</strong>) The username of the CyberArk user to request a password from.</td>
<td>yes, for <strong>Username</strong></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Domain</td>
<td>(If Get credential by is set to Username) The domain to which the username belongs, if applicable.</td>
<td>no</td>
</tr>
<tr>
<td>Safe</td>
<td>(If Get credential by is set to Username) The CyberArk safe the credential should be retrieved from.</td>
<td>yes, for Username</td>
</tr>
<tr>
<td>Account Name</td>
<td>(If Get credential by is set to Identifier) The unique account name or identifier assigned to the CyberArk API credential.</td>
<td>yes, for Identifier</td>
</tr>
<tr>
<td>Use SSL</td>
<td>If enabled, the scanner uses SSL through IIS for secure communications. Enable this option if CyberArk is configured to support SSL through IIS.</td>
<td>no</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>If enabled, the scanner validates the SSL certificate. Enable this option if CyberArk is configured to support SSL through IIS and you want to validate the certificate.</td>
<td>no</td>
</tr>
</tbody>
</table>

**CyberArk (Legacy)**

CyberArk is a popular enterprise password vault that helps you manage privileged credentials. Tenable.io can get credentials from CyberArk to use in a scan.

<table>
<thead>
<tr>
<th>Option</th>
<th>Database Types</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>All</td>
<td>The target system’s username.</td>
<td>yes</td>
</tr>
<tr>
<td>Central Credential Provider Host</td>
<td>All</td>
<td>The CyberArk Central Credential Provider IP/DNS address.</td>
<td>yes</td>
</tr>
<tr>
<td>Option</td>
<td>Database Types</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Central Credential Provider Port</td>
<td>All</td>
<td>The port on which the CyberArk Central Credential Provider is listening.</td>
<td>yes</td>
</tr>
<tr>
<td>CyberArk AIM Service URL</td>
<td>All</td>
<td>The URL of the AIM service. By default, this field uses /AIMWebservice/v1.1/AIM.asmx.</td>
<td>no</td>
</tr>
<tr>
<td>Central Credential Provider Username</td>
<td>All</td>
<td>If the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.</td>
<td>no</td>
</tr>
<tr>
<td>Central Credential Provider Password</td>
<td>All</td>
<td>If the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.</td>
<td>no</td>
</tr>
<tr>
<td>CyberArk Safe</td>
<td>All</td>
<td>The safe on the CyberArk Central Credential Provider server that contained the authentication information you would like to retrieve.</td>
<td>no</td>
</tr>
<tr>
<td>CyberArk Client Certificate</td>
<td>All</td>
<td>The file that contains the PEM certificate used to communicate with the CyberArk host.</td>
<td>no</td>
</tr>
<tr>
<td>CyberArk Client Certificate Private Key</td>
<td>All</td>
<td>The file that contains the PEM private key for the client certificate.</td>
<td>no</td>
</tr>
<tr>
<td>CyberArk Client Certificate Private Key Passphrase</td>
<td>All</td>
<td>The passphrase for the private key, if your authentication implementation requires it.</td>
<td>no</td>
</tr>
<tr>
<td>Option</td>
<td>Database Types</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>CyberArk AppId</td>
<td>All</td>
<td>The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.</td>
<td>yes</td>
</tr>
<tr>
<td>CyberArk Folder</td>
<td>All</td>
<td>The folder on the CyberArk Central Credential Provider server that contains the authentication information you would like to retrieve.</td>
<td>no</td>
</tr>
<tr>
<td>CyberArk Account Details Name</td>
<td>All</td>
<td>The unique name of the credential you want to retrieve from CyberArk.</td>
<td>yes</td>
</tr>
<tr>
<td>PolicyId</td>
<td>All</td>
<td>The PolicyID assigned to the credentials that you want to retrieve from the CyberArk Central Credential Provider.</td>
<td>no</td>
</tr>
<tr>
<td>Use SSL</td>
<td>All</td>
<td>If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.</td>
<td>no</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>All</td>
<td>If CyberArk Central Credential Provider is configured to support SSL through IIS and you want to validate the certificate, select this option. Refer to the custom_CA.inc documentation for how to use self-signed certificates.</td>
<td>no</td>
</tr>
<tr>
<td>Database Port</td>
<td>All</td>
<td>The port on which Tenable.io communicates with the database.</td>
<td>yes</td>
</tr>
<tr>
<td>Database Name</td>
<td>DB2</td>
<td>The name of the database.</td>
<td>no</td>
</tr>
<tr>
<td>Option</td>
<td>Database Types</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Auth type</td>
<td>PostgreSQL</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Oracle</td>
<td>SQL Server values include:</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>SQL Server</td>
<td>• Windows</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sybase ASE</td>
<td>• SQL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Oracle values include:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SYSDBA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SYSOPER</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NORMAL</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sybase ASE values include:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Plain Text</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instance Name</td>
<td>SQL Server</td>
<td>The name for your database instance.</td>
<td>no</td>
</tr>
<tr>
<td>Service type</td>
<td>Oracle</td>
<td>Valid values include:</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>• SID</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SERVICE_NAME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Oracle</td>
<td>The SID value for your database instance or a SERVICE_NAME value. The Service value you enter must match your parameter selection for the Service Type option.</td>
<td>no</td>
</tr>
</tbody>
</table>

HashiCorp Vault

HashiCorp Vault is a popular enterprise password vault that helps you manage privileged credentials. Tenable.io can get credentials from HashiCorp Vault to use in a scan.
<table>
<thead>
<tr>
<th>Option</th>
<th>Database Types</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hashicorp Vault host</td>
<td>All</td>
<td>The Hashicorp Vault IP address or DNS address.</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> If your Hashicorp Vault installation is in a subdirectory, you must include the subdirectory path. For example, type <code>IP address or hostname / subdirectory path</code>.</td>
<td></td>
</tr>
<tr>
<td>Hashicorp Vault port</td>
<td>All</td>
<td>The port on which Hashicorp Vault listens.</td>
<td>yes</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>All</td>
<td>Specifies the authentication type for connecting to the instance: <strong>App Role</strong> or <strong>Certificates</strong>. If you select <strong>Certificates</strong>, additional options for <strong>Hashicorp Client Certificate</strong> and <strong>Hashicorp Client Certificate Private Key</strong> appear. Click <strong>Add File</strong> to select the appropriate files for the client certificate and private key.</td>
<td>yes</td>
</tr>
<tr>
<td>Role ID</td>
<td>All</td>
<td>The GUID provided by Hashicorp Vault when you configured your App Role.</td>
<td>yes</td>
</tr>
<tr>
<td>Role Secret ID</td>
<td>All</td>
<td>The GUID generated by Hashicorp Vault when</td>
<td>yes</td>
</tr>
<tr>
<td>Feature</td>
<td>Scope</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Authentication URL</td>
<td>All</td>
<td>The URL Tenable.io uses to access Hashicorp Vault.</td>
<td>yes</td>
</tr>
<tr>
<td>Username Source</td>
<td>All</td>
<td>A drop-down box to specify if the username is input manually or pulled from Hashicorp Vault.</td>
<td>yes</td>
</tr>
<tr>
<td>Username Key</td>
<td>All</td>
<td>The name in Hashicorp Vault that usernames are stored under.</td>
<td>yes</td>
</tr>
<tr>
<td>Password Key</td>
<td>All</td>
<td>The key in Hashicorp Vault that passwords are stored under.</td>
<td>yes</td>
</tr>
<tr>
<td>Secret Name</td>
<td>All</td>
<td>The key secret you want to retrieve values for.</td>
<td>yes</td>
</tr>
<tr>
<td>Use SSL</td>
<td>All</td>
<td>When enabled, Tenable.io uses SSL through IIS for secure communications. You must configure SSL through IIS in Hashicorp Vault before enabling this option.</td>
<td>no</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>All</td>
<td>When enabled, Tenable.io validates the SSL certificate. You must configure SSL through IIS in Hashicorp Vault before</td>
<td>no</td>
</tr>
</tbody>
</table>
### Database Port
- **All**
- The port on which Ten-able.io communicates with the database.
- **yes**

### Auth Type
- **Oracle**
- The authentication method for the database credentials.
- Valid values include:
  - SYSDBA
  - SYSOPER
  - NORMAL
- **yes**

### Service Type
- **Oracle**
- Valid values include:
  - SID
  - SERVICE_NAME
- **yes**

### Service
- **Oracle**
- The SID value for your database instance or a SERVICE_NAME value.
- The **Service** value you enter must match your parameter selection for the **Service Type** option.
- **yes**

## Lieberman

Lieberman is a popular enterprise password vault that helps you manage privileged credentials. Ten-able.io can get credentials from Lieberman to use in a scan.
<table>
<thead>
<tr>
<th>Option</th>
<th>Database Type</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>All</td>
<td>The target system’s username.</td>
<td>yes</td>
</tr>
<tr>
<td>Lieberman host</td>
<td>All</td>
<td>The Lieberman IP/DNS address.</td>
<td>yes</td>
</tr>
<tr>
<td>Note: If your Lieberman installation is in a subdirectory, you must include the subdirectory path. For example, type <strong>IP address or hostname / subdirectory path</strong>.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lieberman port</td>
<td>All</td>
<td>The port on which Lieberman listens.</td>
<td>yes</td>
</tr>
<tr>
<td>Lieberman API URL</td>
<td>All</td>
<td>The URL Tenable.io uses to access Lieberman.</td>
<td>no</td>
</tr>
<tr>
<td>Lieberman user</td>
<td>All</td>
<td>The Lieberman explicit user for authenticating to the Lieberman API.</td>
<td>yes</td>
</tr>
<tr>
<td>Lieberman password</td>
<td>All</td>
<td>The password for the Lieberman explicit user.</td>
<td>yes</td>
</tr>
<tr>
<td>Lieberman Authenticator</td>
<td>All</td>
<td>The alias used for the authenticator in Lieberman. The name should match the name used in Lieberman.</td>
<td>no</td>
</tr>
<tr>
<td>Note: If you use this option, append a domain to the <strong>Lieberman user</strong> option, i.e., <strong>domain\user</strong>.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lieberman Client Certificate</td>
<td>All</td>
<td>The file that contains the PEM certificate used to communicate with the Lieberman host.</td>
<td>no</td>
</tr>
<tr>
<td>Note: If you use this option, you do not have to enter information in the <strong>Lieberman user</strong>, <strong>Lieberman password</strong>, and <strong>Lieberman Authenticator</strong> fields.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lieberman Client</td>
<td>All</td>
<td>The file that contains the PEM private.</td>
<td>no</td>
</tr>
<tr>
<td>Option</td>
<td>Database Type</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Certificate Private Key</td>
<td></td>
<td>key for the client certificate.</td>
<td></td>
</tr>
<tr>
<td>Lieberman Client Certificate Private</td>
<td>All</td>
<td>The passphrase for the private key, if required.</td>
<td>no</td>
</tr>
<tr>
<td>Key Passphrase</td>
<td></td>
<td>If Lieberman is configured to support SSL through IIS, check for secure</td>
<td>no</td>
</tr>
<tr>
<td>communication.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use SSL</td>
<td>All</td>
<td>If Lieberman is configured to support SSL through IIS and you want to</td>
<td>no</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>All</td>
<td>validate the certificate, check this option. Refer to Custom CA</td>
<td>no</td>
</tr>
<tr>
<td>System Name</td>
<td>All</td>
<td>In the rare case your organization uses one default Lieberman entry for all</td>
<td>no</td>
</tr>
<tr>
<td>managed systems, enter the default</td>
<td></td>
<td>entry name.</td>
<td></td>
</tr>
<tr>
<td>Database Port</td>
<td>All</td>
<td>The port on which Tenable.io communicates with the database.</td>
<td>yes</td>
</tr>
<tr>
<td>Database Name</td>
<td>DB2</td>
<td>(PostgreSQL and DB2 databases only) The name of the database.</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>PostgreSQL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auth type</td>
<td>Oracle</td>
<td>(SQL Server, Oracle. and Sybase ASE databases only) SQL Server values</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>SQL Server</td>
<td>include:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sybase ASE</td>
<td>• Windows</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SQL</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Database Type</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Instance Name</td>
<td>SQL Server</td>
<td>The name for your database instance.</td>
<td>no</td>
</tr>
<tr>
<td>Service type</td>
<td>Oracle</td>
<td>Valid values include:</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- SID</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- SERVICE_NAME</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Oracle</td>
<td>The SID value for your database instance or a SERVICE_NAME value. The <strong>Service</strong> value you enter must match your parameter selection for the <strong>Service Type</strong> option.</td>
<td>no</td>
</tr>
</tbody>
</table>

Oracle values include:
- SYSDBA
- SYSOPER
- NORMAL

Sybase ASE values include:
- RSA
- Plain Text
Host

Tenable.io supports the following forms of host authentication:

- [SNMPv3](#)
- [Secure Shell (SSH)](#)
- [Windows](#)

**SNMPv3**

Use SNMPv3 credentials to scan remote systems that use an encrypted network management protocol (including network devices). Tenable.io uses these credentials to scan for patch auditing or compliance checks.

Click [SNMPv3](#) in the **Credentials** list to configure the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username for the SNMPv3 based account that Tenable.io uses to perform the checks on the target system.</td>
<td>yes</td>
</tr>
<tr>
<td>Port</td>
<td>The port on which SNMP is running on the target system. By default, this value is 161.</td>
<td>no</td>
</tr>
<tr>
<td>Security level</td>
<td>The security level for SNMP:</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>- No authentication and no privacy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Authentication without privacy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Authentication with privacy</td>
<td></td>
</tr>
<tr>
<td>Authentication algorithm</td>
<td>The algorithm the remove service supports (MD5 or SHA1).</td>
<td>yes (if you select authentication)</td>
</tr>
<tr>
<td>Authentication password</td>
<td>The password for the username specified.</td>
<td>yes (if you select authentication)</td>
</tr>
<tr>
<td>Privacy algorithm</td>
<td>The encryption algorithm to use for SNMP traffic.</td>
<td>yes (if you select authentication)</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Privacy password</td>
<td>A password used to protect encrypted SNMP com-</td>
<td>yes (if you select authentication with privacy)</td>
</tr>
<tr>
<td></td>
<td>munication.</td>
<td></td>
</tr>
</tbody>
</table>

## SSH

Use SSH credentials for host-based checks on Unix systems and supported network devices. Tenable.io uses these credentials to obtain local information from remote Unix systems for patch auditing or compliance checks. Tenable.io uses Secure Shell (SSH) protocol version 2 based programs (e.g., OpenSSH, Solaris SSH, etc.) for host-based checks.

Tenable.io encrypts the data to protect it from being viewed by sniffer programs.

**Note:** Non-privileged users with local access on Linux systems can determine basic security issues, such as patch levels or entries in the `/etc/passwd` file. For more comprehensive information, such as system configuration data or file permissions across the entire system, an account with root privileges is required.

**Note:** You can add up to 1000 SSH credentials in a single scan. For best performance, Tenable recommends adding no more than 10 SSH credentials per scan.

Select **SSH** in the **Credentials** list to configure the settings for the following SSH authentication methods:

**SSH Authentication Method: Public Key**

Public Key Encryption, also referred to as asymmetric key encryption, provides a more secure authentication mechanism by the use of a public and private key pair. In asymmetric cryptography, the public key is used to encrypt data and the private key is used to decrypt it. The use of public and private keys is a more secure and flexible method for SSH authentication. Tenable.io supports both DSA and RSA key formats.
Like Public Key Encryption, Tenable.io supports RSA and DSA OpenSSH certificates. Tenable.io also requires the user certificate, which is signed by a Certificate Authority (CA), and the user’s private key.

**Note:** Tenable.io supports the OpenSSH SSH public key format. Formats from other SSH applications, including PuTTY and SSH Communications Security, must be converted to OpenSSH public key format.

The most effective credentialed scans are when the supplied credentials have root privileges. Since many sites do not permit a remote login as root, Tenable.io can invoke su, sudo, su+sudo, dzdo, .k5login, or pbrun with a separate password for an account that has been set up to have su or sudo privileges. In addition, Tenable.io can escalate privileges on Cisco devices by selecting Cisco ‘enable’ or .k5login for Kerberos logins.

**Note:** Tenable.io supports the blowfish-cbc, aes-cbc, and aes-ctr cipher algorithms. Some commercial variants of SSH do not have support for the blowfish algorithm, possibly for export reasons. It is also possible to configure an SSH server to only accept certain types of encryption. Check your SSH server to ensure the correct algorithm is supported.

Tenable.io encrypts all passwords stored in policies. However, the use of SSH keys for authentication rather than SSH passwords is recommended. This helps ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a log in to a system that may not be under your control.

**Note:** For supported network devices, Tenable.io only supports the network device’s username and password for SSH connections.

If an account other than root must be used for privilege escalation, it can be specified under the Escalation account with the Escalation password.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username to authenticate to the host.</td>
<td>yes</td>
</tr>
<tr>
<td>Private Key</td>
<td>The RSA or DSA Open SSH key file of the user.</td>
<td>yes</td>
</tr>
<tr>
<td>Private key passphrase</td>
<td>The passphrase of the Private Key.</td>
<td>no</td>
</tr>
</tbody>
</table>
### Elevate privileges with
The privilege escalation method you want to use to increase users' privileges after initial authentication. Your selection determines the specific options you must configure. For more information, see Privilege Escalation.

### SSH Authentication Method: Certificate

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username to authenticate to the host.</td>
<td>yes</td>
</tr>
<tr>
<td>User Certificate</td>
<td>The RSA or DSA Open SSH certificate file of the user.</td>
<td>yes</td>
</tr>
<tr>
<td>Private Key</td>
<td>The RSA or DSA Open SSH key file of the user.</td>
<td>yes</td>
</tr>
<tr>
<td>Private key passphrase</td>
<td>The passphrase of the Private Key.</td>
<td>no</td>
</tr>
<tr>
<td>Elevate privileges with</td>
<td>The privilege escalation method you want to use to increase users' privileges after initial authentication. Your selection determines the specific options you must configure. For more information, see Privilege Escalation.</td>
<td>no</td>
</tr>
</tbody>
</table>

### SSH Authentication Method: CyberArk Vault

CyberArk is a popular enterprise password vault that helps you manage privileged credentials. Tenable.io can get credentials from CyberArk to use in a scan.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username of the target system.</td>
<td>yes</td>
</tr>
<tr>
<td>CyberArk AIM Service URL</td>
<td>The URL for the CyberArk AIM web service. By default, Tenable.io uses /AIMWeb-service/v1.1/AIM.asmx.</td>
<td>no</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Central Credential Provider Host</td>
<td>The CyberArk Central Credential Provider IP/DNS address.</td>
<td>yes</td>
</tr>
<tr>
<td>Central Credential Provider Port</td>
<td>The port on which the CyberArk Central Credential Provider is listening.</td>
<td>yes</td>
</tr>
<tr>
<td>Central Credential Provider Username</td>
<td>The username of the vault, if the CyberArk Central Credential Provider is configured to use basic authentication.</td>
<td>no</td>
</tr>
<tr>
<td>Central Credential Provider Password</td>
<td>The password of the vault, if the CyberArk Central Credential Provider is configured to use basic authentication.</td>
<td>no</td>
</tr>
<tr>
<td>Safe</td>
<td>The safe on the CyberArk Central Credential Provider server that contained the authentication information that you want to retrieve.</td>
<td>yes</td>
</tr>
<tr>
<td>CyberArk Client Certificate</td>
<td>The file that contains the PEM certificate used to communicate with the CyberArk host.</td>
<td>no</td>
</tr>
<tr>
<td>CyberArk Client Certificate Private Key</td>
<td>The file that contains the PEM private key for the client certificate.</td>
<td>no</td>
</tr>
<tr>
<td>CyberArk Client Certificate Private Key Passphrase</td>
<td>The passphrase for the private key, if required.</td>
<td>no</td>
</tr>
<tr>
<td>AppId</td>
<td>The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target</td>
<td>yes</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Folder</td>
<td>The folder on the CyberArk Central Credential Provider server that contains the authentication information that you want to retrieve.</td>
<td>yes</td>
</tr>
<tr>
<td>PolicyId</td>
<td>The PolicyID assigned to the credentials that you want to retrieve from the CyberArk Central Credential Provider.</td>
<td>no</td>
</tr>
<tr>
<td>Use SSL</td>
<td>If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.</td>
<td>no</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>If CyberArk Central Credential Provider is configured to support SSL through IIS and you want to validate the certificate check this. Refer to custom_CA.inc documentation for how to use self-signed certificates.</td>
<td>no</td>
</tr>
<tr>
<td>CyberArk Account Details Name</td>
<td>The unique name of the credential you want to retrieve from CyberArk.</td>
<td>no</td>
</tr>
<tr>
<td>CyberArk Address</td>
<td>The domain for the user account.</td>
<td>no</td>
</tr>
<tr>
<td>CyberArk elevate privileges with</td>
<td>The privilege escalation method you want to use to increase users' privileges after initial authentication. Your selection determines the specific options you must configure. For more information, see <a href="#">Privilege Escalation</a>.</td>
<td>no</td>
</tr>
<tr>
<td>Custom password prompt</td>
<td>The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to Tenable.io receiving an unrecognized password prompt on the target host's interactive SSH shell.</td>
<td>no</td>
</tr>
</tbody>
</table>

**SSH Authentication Method:** Hashicorp Vault
HashiCorp Vault is a popular enterprise password vault that helps you manage privileged credentials. Tenable.io can retrieve credentials from HashiCorp Vault to use in a scan.

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hashicorp Vault host</td>
<td>(Required) The Hashicorp Vault IP address or DNS address.</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If your Hashicorp Vault installation is in a subdirectory, you must include the subdirectory path. For example, type IP address or hostname/subdirectory path.</td>
<td></td>
</tr>
<tr>
<td>Hashicorp Vault port</td>
<td>(Required) The port on which Hashicorp Vault listens.</td>
<td>yes</td>
</tr>
<tr>
<td>Hashicorp Vault API URL</td>
<td>The URL Tenable.io uses to access Hashicorp Vault.</td>
<td>yes</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Specifies the authentication type for connecting to the instance: <strong>App Role</strong> or <strong>Certificates</strong>.</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>If you select <strong>Certificates</strong>, additional options for <strong>Hashicorp Client Certificate</strong> and <strong>Hashicorp Client Certificate Private Key</strong> appear. Click <strong>Add File</strong> to select files for the client certificate and private key.</td>
<td></td>
</tr>
<tr>
<td>Role ID</td>
<td>Required if you select App Role for <strong>Authentication Type</strong>. The GUID provided by Hashicorp Vault when you configured your App Role.</td>
<td>yes</td>
</tr>
<tr>
<td>Role Secret ID</td>
<td>Required if you select App Role for <strong>Authentication Type</strong>. The GUID generated by Hashicorp Vault when you configured your App Role.</td>
<td>yes</td>
</tr>
<tr>
<td>Authentication URL</td>
<td>The URL Tenable.io uses to access Hashicorp Vault.</td>
<td>yes</td>
</tr>
<tr>
<td>Namespace</td>
<td>The name of a specified team in a multi-team environment.</td>
<td>no</td>
</tr>
</tbody>
</table>
For more information about multi-team environments, see the Hashicorp documentation.

| KV Engine URL | The URL Tenable.io uses to access the Hashicorp Vault secrets engine. | yes |
| Username Source | Specifies if the username is input manually or pulled from Hashicorp Vault. | yes |
| Username Key | The name in Hashicorp Vault that usernames are stored under. | yes |
| Password Key | The key in Hashicorp Vault that passwords are stored under. | yes |
| Secret Name | The key secret you want to retrieve values for. | yes |
| Use SSL | When enabled, Tenable.io uses SSL through IIS for secure communications. You must configure SSL through IIS in Hashicorp Vault before enabling this option. | no |
| Verify SSL | When enabled, Tenable.io validates the SSL certificate. You must configure SSL through IIS in Hashicorp Vault before enabling this option. | no |

**SSH Authentication Method: Kerberos**

Kerberos, developed by MIT’s Project Athena, is a client/server application that uses a symmetric key encryption protocol. In symmetric encryption, the key used to encrypt the data is the same as the key used to decrypt the data. Organizations deploy a KDC (Key Distribution Center) that contains all users and services that require Kerberos authentication. Users authenticate to Kerberos by requesting a TGT (Ticket Granting Ticket). Once a user is granted a TGT, it can be used to request service tickets from the KDC to be able to utilize other Kerberos based services. Kerberos uses the CBC (Cipher Block Chain) DES encryption protocol to encrypt all communications.

*Note:* You must already have a Kerberos environment established to use this method of authentication.
The Tenable.io implementation of Unix-based Kerberos authentication for SSH supports the aes-cbc and aes-ctr encryption algorithms. An overview of how Tenable.io interacts with Kerberos is as follows:

1. The end-user gives the IP of the KDC.
2. The nessusd asks sshd if it supports Kerberos authentication.
3. The sshd says yes.
4. The nessusd requests a Kerberos TGT, along with login and password.
5. Kerberos sends a ticket back to nessusd.
6. The nessusd gives the ticket to sshd.
7. The nessusd is logged in.

In both Windows and SSH credentials settings, you can specify credentials using Kerberos keys from a remote system. Note that there are differences in the configurations for Windows and SSH.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username of the target system.</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>The password of the username specified.</td>
<td>yes</td>
</tr>
<tr>
<td>Key Distribution Center (KDC)</td>
<td>This host supplies the session tickets for the user.</td>
<td>yes</td>
</tr>
<tr>
<td>KDC Port</td>
<td>Directs Tenable.io to connect to the KDC if it is running on a port other than 88.</td>
<td>no</td>
</tr>
<tr>
<td>KDC Transport</td>
<td>The method by which you want to access the KDC server.</td>
<td>no</td>
</tr>
</tbody>
</table>

**Note:** if you set **KDC Transport** to **UDP**, you may also need to change the port number, because depending on the implementation, the KDC UDP protocol uses either port 88 or 750 by default.
If Kerberos is used, ssqd must be configured with Kerberos support to verify the ticket with the KDC. Reverse DNS lookups must be properly configured for this to work. The Kerberos interaction method must be gssapi-with-mic.

**SSH Authentication Method: Password**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username of the target system.</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>The password of the username specified.</td>
<td>yes</td>
</tr>
<tr>
<td>Elevate privileges with</td>
<td>The privilege escalation method you want to use to increase users' privileges after initial authentication. Your selection determines the specific options you must configure. For more information, see Privilege Escalation.</td>
<td>no</td>
</tr>
</tbody>
</table>

| Custom password prompt  | The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to Tenable.io receiving an unrecognized password prompt on the target host's interactive SSH shell. | no       |

**SSH Authentication Method: Lieberman RED**

Lieberman is a popular enterprise password vault that helps you manage privileged credentials. Tenable.io can get credentials from Lieberman to use in a scan.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The target system’s username.</td>
<td>yes</td>
</tr>
<tr>
<td>Lieberman host</td>
<td>The Lieberman IP/DNS address.</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>Note: If your Lieberman installation is in a subdirectory, you must include the subdirectory path. For example, type IP address or hostname / subdirectory path.</td>
<td></td>
</tr>
<tr>
<td>Lieberman port</td>
<td>The port on which Lieberman listens.</td>
<td>yes</td>
</tr>
<tr>
<td>Lieberman API URL</td>
<td>The URL Tenable.io uses to access Lieberman.</td>
<td>no</td>
</tr>
<tr>
<td>Lieberman user</td>
<td>The Lieberman explicit user for authenticating to the Lieberman RED API.</td>
<td>yes</td>
</tr>
<tr>
<td>Lieberman password</td>
<td>The password for the Lieberman explicit user.</td>
<td>yes</td>
</tr>
<tr>
<td>Lieberman Authenticator</td>
<td>The alias used for the authenticator in Lieberman. The name should match the name used in Lieberman.</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>Note: If you use this option, append a domain to the Lieberman user option, i.e., domain\user.</td>
<td></td>
</tr>
<tr>
<td>Lieberman Client Certificate</td>
<td>The file that contains the PEM certificate used to communicate with the Lieberman host.</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>Note: If you use this option, you do not have to enter information in the Lieberman user, Lieberman password, and Lieberman Authenticator fields.</td>
<td></td>
</tr>
<tr>
<td>Lieberman Client Certificate Private Key</td>
<td>The file that contains the PEM private key for the client certificate.</td>
<td>no</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Lieberman Client Certificate Private Key Passphrase</td>
<td>The passphrase for the private key, if required.</td>
<td>no</td>
</tr>
<tr>
<td>Use SSL</td>
<td>If Lieberman is configured to support SSL through IIS, check for secure communication.</td>
<td>no</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>If Lieberman is configured to support SSL through IIS and you want to validate the certificate, check this option. Refer to Custom CA documentation for how to use self-signed certificates.</td>
<td>no</td>
</tr>
<tr>
<td>System Name</td>
<td>In the rare case your organization uses one default Lieberman entry for all managed systems, enter the default entry name.</td>
<td>no</td>
</tr>
<tr>
<td>Custom password prompt</td>
<td>The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to Tenable.io receiving an unrecognized password prompt on the target host's interactive SSH shell.</td>
<td>no</td>
</tr>
</tbody>
</table>

**SSH Authentication Method: Thycotic Secret Server**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username to authenticate via SSH to the system.</td>
<td>yes</td>
</tr>
<tr>
<td>Thycotic Secret Name</td>
<td>The value of the secret on the Thycotic server. The secret is labeled <strong>Secret Name</strong> on the Thycotic server.</td>
<td>yes</td>
</tr>
<tr>
<td>Thycotic Secret Server URL</td>
<td>The transfer method, target , and target directory for the scanner. You can find this value on the Thycotic server in <strong>Admin &gt; Configuration &gt; Application Settings &gt; Secret Server URL</strong>.</td>
<td>yes</td>
</tr>
</tbody>
</table>
For example, consider the following address:

- Transfer method: **https** indicates an ssl connection.
- Target: **pw.mydomain.com** is the target address.
- Target Directory: **/SecretServer/** is the root directory.

<table>
<thead>
<tr>
<th>Thycotic Login Name</th>
<th>The username to authenticate to the Thycotic server.</th>
<th>yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thycotic Password</td>
<td>The password to authenticate to the Thycotic server.</td>
<td>yes</td>
</tr>
<tr>
<td>Thycotic Organization</td>
<td>The organization you want to query. You can use this value for cloud instances of Thycotic.</td>
<td>no</td>
</tr>
<tr>
<td>Thycotic Domain</td>
<td>The domain of the Thycotic server.</td>
<td>no</td>
</tr>
<tr>
<td>Use Private Key</td>
<td>The key for the SSH connection, if you do not use a password.</td>
<td>no</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>Whether you want to verify if the SSL Certificate on the server is signed by a trusted CA.</td>
<td>no</td>
</tr>
<tr>
<td>Thycotic elevate privileges with</td>
<td>The privilege escalation method you want to use to increase users' privileges after initial authentication. Multiple options for privilege escalation are supported, including su, su+sudo and sudo. Your selection determines the specific options you must configure. For more information, see <a href="#">Privilege Escalation</a>.</td>
<td>no</td>
</tr>
<tr>
<td>Custom password prompt</td>
<td>The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to</td>
<td>no</td>
</tr>
</tbody>
</table>
Tenable.io receiving an unrecognized password prompt on the target host's interactive SSH shell.

### SSH Authentication Method: BeyondTrust

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username to log in to the hosts you want to scan.</td>
<td>yes</td>
</tr>
<tr>
<td>BeyondTrust host</td>
<td>The BeyondTrust IP address or DNS address.</td>
<td>yes</td>
</tr>
<tr>
<td>BeyondTrust port</td>
<td>The port on which BeyondTrust listens.</td>
<td>yes</td>
</tr>
<tr>
<td>BeyondTrust API user</td>
<td>The API user provided by BeyondTrust.</td>
<td>yes</td>
</tr>
<tr>
<td>BeyondTrust API key</td>
<td>The API key provided by BeyondTrust.</td>
<td>yes</td>
</tr>
<tr>
<td>Checkout duration</td>
<td>The length of time, in minutes, that you want to keep credentials checked out in BeyondTrust. Configure the Checkout duration to exceed the typical duration of your Tenable.io scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails.</td>
<td>yes</td>
</tr>
</tbody>
</table>

**Note:** Configure the password change interval in BeyondTrust so that password changes do not disrupt your Tenable.io scans. If BeyondTrust changes a password during a scan, the scan fails.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use SSL</td>
<td>When enabled, Tenable.io uses SSL through IIS for secure communications. You must configure SSL through IIS in BeyondTrust before enabling this option.</td>
<td>no</td>
</tr>
<tr>
<td>Verify SSL certificate</td>
<td>When enabled, Tenable.io validates the SSL certificate. You must configure SSL through IIS in BeyondTrust</td>
<td>no</td>
</tr>
</tbody>
</table>
before enabling this option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use private key</td>
<td></td>
<td>When enabled, Tenable.io uses private key-based authentication for SSH connections instead of password authentication. If it fails, the password is requested.</td>
</tr>
<tr>
<td>Use privilege escalation</td>
<td>no</td>
<td>When enabled, BeyondTrust uses the configured privilege escalation command. If it returns something, it will use it for the scan.</td>
</tr>
<tr>
<td>Custom password prompt</td>
<td>no</td>
<td>The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to Tenable.io receiving an unrecognized password prompt on the target host's interactive SSH shell.</td>
</tr>
</tbody>
</table>

**Scan-wide Credential Type Settings for SSH**

These settings apply to all SSH-type credentials in the current scan. You can edit these settings in any instance of the credential type in the current scan; your changes automatically apply to the other credentials of that type in the scan.

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>known_hosts file</td>
<td>None</td>
<td>If you upload an SSH known_hosts file, Tenable.io only attempts to log in to hosts in this file. This can ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a log into a system that may not be under your control.</td>
</tr>
<tr>
<td>Preferred port</td>
<td>22</td>
<td>The port on which SSH is running on the target system.</td>
</tr>
<tr>
<td>Client version</td>
<td>OpenSSH_5.0</td>
<td>The type of SSH client Tenable.io impersonates while scanning.</td>
</tr>
<tr>
<td>Attempt least privilege</td>
<td>Cleared</td>
<td>Enables or disables dynamic privilege escalation. When enabled, Tenable.io attempts to run the scan with an</td>
</tr>
</tbody>
</table>
account with lesser privileges, even if the **Elevate privileges with** option is enabled. If a command fails, Tenable.io escalates privileges. Plugins 101975 and 101976 report which plugins ran with or without escalated privileges.

**Note:** Enabling this option may increase scan run time by up to 30%.

**Note:** Non-privileged users with local access on Unix systems can determine basic security issues, such as patch levels or entries in the `/etc/passwd` file. For more comprehensive information, such as system configuration data or file permissions across the entire system, an account with root privileges is required.

### Windows

Click **Windows** in the **Credentials** list to configure settings for the Windows-based authentication methods described below.

#### Windows Authentication Method: CyberArk Vault

CyberArk is a popular enterprise password vault that helps you manage privileged credentials. Tenable.io can get credentials from CyberArk to use in a scan.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username of the target system.</td>
<td>yes</td>
</tr>
<tr>
<td>CyberArk AIM Service URL</td>
<td>The URL for the CyberArk AIM web service. By default, Tenable.io uses <code>/AIMWebservice/v1.1/AIM.asmx</code>.</td>
<td>no</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain to which the username belongs.</td>
<td>no</td>
</tr>
<tr>
<td>Central Credential Provider Host</td>
<td>The CyberArk Central Credential Provider IP/DNS address.</td>
<td>yes</td>
</tr>
</tbody>
</table>

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider Port</td>
<td>The username of the vault, if the CyberArk Central Credential Provider is configured to use basic authentication.</td>
<td>no</td>
</tr>
<tr>
<td>Central Credential Provider Username</td>
<td>The password of the vault, if the CyberArk Central Credential Provider is configured to use basic authentication.</td>
<td>no</td>
</tr>
<tr>
<td>Safe</td>
<td>The safe on the CyberArk Central Credential Provider server that contained the authentication information that you want to retrieve.</td>
<td>yes</td>
</tr>
<tr>
<td>CyberArk Client Certificate</td>
<td>The file that contains the PEM certificate used to communicate with the CyberArk host.</td>
<td>no</td>
</tr>
<tr>
<td>CyberArk Client Certificate Private Key</td>
<td>The file that contains the PEM private key for the client certificate.</td>
<td>no</td>
</tr>
<tr>
<td>CyberArk Client Certificate Private Key Passphrase</td>
<td>The passphrase for the private key, if required.</td>
<td>no</td>
</tr>
<tr>
<td>AppId</td>
<td>The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.</td>
<td>yes</td>
</tr>
<tr>
<td>Folder</td>
<td>The folder on the CyberArk Central Credential Provider server that contains the authentication information that you want to retrieve.</td>
<td>yes</td>
</tr>
<tr>
<td>PolicyId</td>
<td>The PolicyID assigned to the credentials that you want to retrieve.</td>
<td>no</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Retrieve from CyberArk</td>
<td>Required to retrieve credentials from the CyberArk Central Credential Provider.</td>
<td>yes</td>
</tr>
<tr>
<td>Use SSL</td>
<td>If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.</td>
<td>no</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>If CyberArk Central Credential Provider is configured to support SSL through IIS and you want to validate the certificate check this. Refer to custom_CA.inc documentation for how to use self-signed certificates.</td>
<td>no</td>
</tr>
<tr>
<td>CyberArk Account Details</td>
<td>The unique name of the credential you want to retrieve from CyberArk.</td>
<td>no</td>
</tr>
</tbody>
</table>

**Windows Authentication Method: Hashicorp Vault**

HashiCorp Vault is a popular enterprise password vault that helps you manage privileged credentials. Tenable.io can retrieve credentials from HashiCorp Vault to use in a scan.

<table>
<thead>
<tr>
<th>Option</th>
<th>Default Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hashicorp Vault host</td>
<td>(Required) The Hashicorp Vault IP address or DNS address.</td>
<td>yes</td>
</tr>
<tr>
<td>Note: If your Hashicorp Vault installation is in a sub-directory, you must include the subdirectory path. For example, type IP address or hostname/subdirectory path.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hashicorp Vault port</td>
<td>The port on which Hashicorp Vault listens.</td>
<td>yes</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Specifies the authentication type for connecting to the instance: <strong>App Role</strong> or <strong>Certificates</strong>.</td>
<td>yes</td>
</tr>
<tr>
<td>If you select <strong>Certificates</strong>, additional options for <strong>Hashicorp Client Certificate</strong> and <strong>Hashicorp Client Certificate Private Key</strong> appear. Click <strong>Add File</strong> to select files for the client certificate and private key.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Role ID</td>
<td>Required if you select <strong>App Role</strong> for <strong>Authentication Type</strong>. The GUID provided by Hashicorp Vault when you configured your App Role.</td>
<td>yes</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>Role Secret ID</td>
<td>Required if you select <strong>App Role</strong> for <strong>Authentication Type</strong>. The GUID generated by Hashicorp Vault when you configured your App Role.</td>
<td>yes</td>
</tr>
<tr>
<td>Authentication URL</td>
<td>The URL Tenable.io uses to access Hashicorp Vault.</td>
<td>yes</td>
</tr>
<tr>
<td>Namespace</td>
<td>The name of a specified team in a multi-team environment. For more information about multi-team environments, see the <a href="#">Hashicorp documentation</a>.</td>
<td>no</td>
</tr>
<tr>
<td>KV Engine URL</td>
<td>The URL Tenable.io uses to access the Hashicorp Vault secrets engine.</td>
<td>yes</td>
</tr>
<tr>
<td>Username Source</td>
<td>Specifies if the username is input manually or pulled from Hashicorp Vault.</td>
<td>yes</td>
</tr>
<tr>
<td>Username Key</td>
<td>The name in Hashicorp Vault that usernames are stored under.</td>
<td>yes</td>
</tr>
<tr>
<td>Password Key</td>
<td>The key in Hashicorp Vault that passwords are stored under.</td>
<td>yes</td>
</tr>
<tr>
<td>Secret Name</td>
<td><em>(Required)</em> The key secret you want to retrieve values for.</td>
<td>yes</td>
</tr>
<tr>
<td>Use SSL</td>
<td>When enabled, Tenable.io uses SSL through IIS for secure communications. You must configure SSL through IIS in Hashicorp Vault before enabling this option.</td>
<td>no</td>
</tr>
<tr>
<td>Verify SSL</td>
<td>When enabled, Tenable.io validates the SSL certificate. You must configure SSL through IIS in Hashicorp Vault before enabling this option.</td>
<td>no</td>
</tr>
</tbody>
</table>

**Windows Authentication Method: Kerberos**
## Windows Authentication Method: Lieberman RED

Lieberman is a popular enterprise password vault that helps you manage privileged credentials. Tenable.io can get credentials from Lieberman to use in a scan.

<table>
<thead>
<tr>
<th>Option</th>
<th>Default</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>None</td>
<td>The target system's username.</td>
<td>yes</td>
</tr>
<tr>
<td>Domain</td>
<td>None</td>
<td>The domain, if the username is part of a domain.</td>
<td>no</td>
</tr>
<tr>
<td>Lieberman host</td>
<td>None</td>
<td>The Lieberman IP/DNS address.</td>
<td>yes</td>
</tr>
</tbody>
</table>

**Note:** If your Lieberman installation is in a subdirectory, you must include the subdirectory.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lieberman port</td>
<td>The port on which Lieberman listens.</td>
<td>yes</td>
</tr>
<tr>
<td>Lieberman API URL</td>
<td>The URL Tenable.io uses to access Lieberman.</td>
<td>no</td>
</tr>
<tr>
<td>Lieberman user</td>
<td>The Lieberman explicit user for authenticating to the Lieberman RED API.</td>
<td>yes</td>
</tr>
<tr>
<td>Lieberman password</td>
<td>The password for the Lieberman explicit user.</td>
<td>yes</td>
</tr>
<tr>
<td>Lieberman Authenticator</td>
<td>The alias used for the authenticator in Lieberman. The name should match the name used in Lieberman.</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you use this option, append a domain to the Lieberman user option, i.e., <code>domain\user</code>.</td>
<td></td>
</tr>
<tr>
<td>Lieberman Client Certificate</td>
<td>The file that contains the PEM certificate used to communicate with the Lieberman host.</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you use this option, you do not have to enter information in the Lieberman user, Lieberman password, and Lieberman Authenticator fields.</td>
<td></td>
</tr>
<tr>
<td>Lieberman Client Certificate Private Key</td>
<td>The file that contains the PEM private key for the client certificate.</td>
<td>no</td>
</tr>
<tr>
<td>Lieberman Client Certificate Private Key Passphrase</td>
<td>The passphrase for the private key, if required.</td>
<td>no</td>
</tr>
<tr>
<td>Use SSL</td>
<td>If Lieberman is configured to support SSL</td>
<td>no</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>through IIS, check for secure communication.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>If Lieberman is configured to support SSL through IIS and you want to validate the certificate, check this. Refer to custom_CA.inc documentation for how to use self-signed certificates.</td>
<td>no</td>
</tr>
<tr>
<td>System Name</td>
<td>In the rare case your organization uses one default Lieberman entry for all managed systems, enter the default entry name.</td>
<td>no</td>
</tr>
</tbody>
</table>

**Windows Authentication Method: LM Hash**

The Lanman authentication method was prevalent on Windows NT and early Windows 2000 server deployments. It is retained for backward compatibility.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username on the target system.</td>
<td>yes</td>
</tr>
<tr>
<td>Hash</td>
<td>The hash you want to use.</td>
<td>yes</td>
</tr>
<tr>
<td>Domain</td>
<td>The Windows domain to which the username belongs.</td>
<td>no</td>
</tr>
</tbody>
</table>

**Windows Authentication Method: NTLM Hash**

The [NTLM authentication method](#), introduced with Windows NT, provided improved security over Lanman authentication. The enhanced version, NTLMv2, is cryptographically more secure than NTLM and is the default authentication method chosen by Tenable.io when attempting to log into a Windows server. NTLMv2 can make use of SMB Signing.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username on the target system.</td>
<td>yes</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Hash</td>
<td>The hash you want to use.</td>
<td>yes</td>
</tr>
<tr>
<td>Domain</td>
<td>The Windows domain to which the username belongs.</td>
<td>no</td>
</tr>
</tbody>
</table>

**Windows Authentication Method: Password**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username on the target system.</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>The user password on the target system.</td>
<td>yes</td>
</tr>
<tr>
<td>Domain</td>
<td>The Windows domain to which the username belongs.</td>
<td>no</td>
</tr>
</tbody>
</table>

**Windows Authentication Method: Thycotic Secret Server**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username to authenticate via SSH to the system.</td>
<td>yes</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain to which the username belongs.</td>
<td>no</td>
</tr>
<tr>
<td>Thycotic Secret Name</td>
<td>The value of the secret on the Thycotic server. The secret is labeled <strong>Secret Name</strong> on the Thycotic server.</td>
<td>yes</td>
</tr>
</tbody>
</table>
| Thycotic Secret Server URL | The transfer method, target, and target directory for the scanner. You can find this value on the Thycotic server in Admin > Configuration > Application Settings > Secret Server URL. For example, consider the following address:  
- **https** indicates an ssl connection.  
- **pw.mydomain.com** is the target address.  
- **/SecretServer/** is the root directory. | yes      |
<p>| Thycotic Login          | The username to authenticate to the Thycotic server.                                                                                                                                                     | yes      |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thycotic Password</td>
<td>The password to authenticate to the Thycotic server.</td>
<td>yes</td>
</tr>
<tr>
<td>Thycotic Organization</td>
<td>The organization you want to query. You can use this value for cloud instances of Thycotic.</td>
<td>no</td>
</tr>
<tr>
<td>Thycotic Domain</td>
<td>The domain of the Thycotic server.</td>
<td>no</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>Whether you want to verify if the SSL Certificate on the server is signed by a trusted CA.</td>
<td>no</td>
</tr>
</tbody>
</table>

**Windows Authentication Method: BeyondTrust**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username to log in to the hosts you want to scan.</td>
<td>yes</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain of the username, if required by BeyondTrust.</td>
<td>no</td>
</tr>
<tr>
<td>BeyondTrust host</td>
<td>The BeyondTrust IP address or DNS address.</td>
<td>yes</td>
</tr>
<tr>
<td>BeyondTrust port</td>
<td>The port on which BeyondTrust listens.</td>
<td>yes</td>
</tr>
<tr>
<td>BeyondTrust API user</td>
<td>The API user provided by BeyondTrust.</td>
<td>yes</td>
</tr>
<tr>
<td>BeyondTrust API key</td>
<td>The API key provided by BeyondTrust.</td>
<td>yes</td>
</tr>
<tr>
<td>Checkout duration</td>
<td>The length of time, in minutes, that you want to keep credentials checked out in BeyondTrust. Configure the Checkout duration to exceed the typical duration of your Tenable.io scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails.</td>
<td>yes</td>
</tr>
</tbody>
</table>
**Note:** Configure the password change interval in BeyondTrust so that password changes do not disrupt your Tenable.io scans. If BeyondTrust changes a password during a scan, the scan fails.

<table>
<thead>
<tr>
<th>Use SSL</th>
<th>When enabled, Tenable.io uses SSL through IIS for secure communications. You must configure SSL through IIS in BeyondTrust before enabling this option.</th>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify SSL certificate</td>
<td>When enabled, Tenable.io validates the SSL certificate. You must configure SSL through IIS in BeyondTrust before enabling this option.</td>
<td>no</td>
</tr>
</tbody>
</table>

**Scan-wide Credential Type Settings for Windows**

These settings apply to all Windows-type credentials in the current scan. You can edit these settings in any instance of the credential type in the current scan; your changes automatically apply to the other credentials of that type in the scan.

<table>
<thead>
<tr>
<th>Option</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never send credentials in the clear</td>
<td>Enabled</td>
<td>By default, for security reasons, this option is enabled.</td>
</tr>
<tr>
<td>Do not use NTLMv1 authentication</td>
<td>Enabled</td>
<td>If the <strong>Do not use NTLMv1 authentication</strong> option is disabled, then it is theoretically possible to trick Tenable.io into attempting to log into a Windows server with domain credentials via the NTLM version 1 protocol. This provides the remote attacker with the ability to use a hash obtained from Tenable.io. This hash can be potentially cracked to reveal a username or password. It may also be used to directly log into other servers. Force Tenable.io to use NTLMv2 by enabling the <strong>Only use NTLMv2</strong> setting at scan time. This prevents a hostile Windows server from using NTLM and receiving a hash. Because NTLMv1 is an insecure protocol, this option is enabled by default.</td>
</tr>
<tr>
<td>Option</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Start the Remote Registry service during the scan</td>
<td>Disabled</td>
<td>This option tells Tenable.io to start the Remote Registry service on computers being scanned if it is not running. This service must be running in order for Tenable.io to execute some Windows local check plugins.</td>
</tr>
<tr>
<td>Enable administrative shares during the scan</td>
<td>Disabled</td>
<td>This option allows Tenable.io to access certain registry entries that can be read with administrator privileges.</td>
</tr>
<tr>
<td>Start the Server service during the scan</td>
<td>Disabled</td>
<td>When enabled, the scanner temporarily enables the Windows Server service, which allows the computer to share files and other devices on a network. The service is disabled after the scan completes. By default, Windows systems have the Windows Server service enabled, which means you do not need to enable this setting. However, if you disable the Windows Server service in your environment, and want to scan using SMB credentials, you must enable this setting so that the scanner can access files remotely.</td>
</tr>
</tbody>
</table>

**Windows Authentication Considerations**

Regarding the authentication methods:

- Tenable.io automatically uses SMB signing if it is required by the remote Windows server. SMB signing is a cryptographic checksum applied to all SMB traffic to and from a Windows server. Many system administrators enable this feature on their servers to ensure that remote users are 100% authenticated and part of a domain. In addition, make sure you enforce a policy that mandates the use of strong passwords that cannot be easily broken via dictionary attacks from tools like John the Ripper and L0phtCrack. Note that there have been many different types of attacks against Windows security to illicit hashes from computers for re-use in attacking servers. SMB Signing adds a layer of security to prevent these man-in-the-middle attacks.
The SPNEGO (Simple and Protected Negotiate) protocol provides Single Sign On (SSO) capability from a Windows client to a variety of protected resources via the users’ Windows login credentials. Tenable.io supports use of SPNEGO Scans and Policies: Scans 54 of 151 with either NTLMSSP with LMv2 authentication or Kerberos and RC4 encryption. SPNEGO authentication happens through NTLM or Kerberos authentication; nothing needs to be set in the Tenable.io scan configuration.

If an extended security scheme (such as Kerberos or SPNEGO) is not supported or fails, Tenable.io attempts to log in via NTLMSSP/LMv2 authentication. If that fails, Tenable.io then attempts to log in using NTLM authentication.

Tenable.io also supports the use of Kerberos authentication in a Windows domain. To configure this, the IP address of the Kerberos Domain Controller (actually, the IP address of the Windows Active Directory Server) must be provided.

Server Message Block (SMB) is a file-sharing protocol that allows computers to share information across the network. Providing this information to Tenable.io allows it to find local information from a remote Windows host. For example, using credentials enables Tenable.io to determine if important security patches have been applied. It is not necessary to modify other SMB parameters from default settings.

The SMB domain field is optional and Tenable.io is able to log on with domain credentials without this field. The username, password, and optional domain refer to an account that the target machine is aware of. For example, given a username of joesmith and a password of my4x4mpl3, a Windows server first looks for this username in the local system’s list of users, and then determines if it is part of a domain.

Regardless of credentials used, Tenable.io always attempts to log into a Windows server with the following combinations:

- Administrator without a password
- A random username and password to test Guest accounts
- No username or password to test null sessions

The actual domain name is only required if an account name is different on the domain from that on the computer. It is entirely possible to have an Administrator account on a Windows server and within the domain. In this case, to log onto the local server, the username of Administrator is used
with the password of that account. To log onto the domain, the Administrator username is also used, but with the domain password and the name of the domain.

When multiple SMB accounts are configured, Tenable.io attempts to log in with the supplied credentials sequentially. Once Tenable.io is able to authenticate with a set of credentials, it checks subsequent credentials supplied, but only uses them if administrative privileges are granted when previous accounts provided user access.

Some versions of Windows allow you to create a new account and designate it as an administrator. These accounts are not always suitable for performing credentialed scans. Tenable recommends that the original administrative account, named Administrator be used for credentialed scanning to ensure full access is permitted. On some versions of Windows, this account may be hidden. The real administrator account can be unhidden by running a DOS prompt with administrative privileges and typing the following command:

```
C:\> net user administrator /active:yes
```

If an SMB account is created with limited administrator privileges, Tenable.io can easily and securely scan multiple domains. Tenable recommends that network administrators create specific domain accounts to facilitate testing. Tenable.io includes a variety of security checks for Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 that are more accurate if a domain account is provided. Tenable.io does attempt to try several checks in most cases if no account is provided.

**Note:** The Windows Remote Registry service allows remote computers with credentials to access the registry of the computer being audited. If the service is not running, reading keys and values from the registry is not possible, even with full credentials. This service must be started for a Tenable.io credentialed scan to fully audit a system using credentials.

For more information, see the Tenable blog post [Dynamic Remote Registry Auditing - Now you see it, now you don’t!](https://www.tenable.com/blog/dynamic-remote-registry-auditing-now-you-see-it-now-you-dont)

Credentialed scans on Windows systems require that a full administrator level account be used. Several bulletins and software updates by Microsoft have made reading the registry to determine software patch level unreliable without administrator privileges, but not all of them. Tenable.io plugins check that the provided credentials have full administrative access to ensure the plugins execute properly. For example, full administrative access is required to perform direct reading of the
file system. This allows Tenable.io to attach to a computer and perform direct file analysis to determine the true patch level of the systems being evaluated.
Privilege Escalation

You can configure privilege escalation for a credentialed scan if the scan uses the following authentication methods:

<table>
<thead>
<tr>
<th>Authentication Methods that Support Escalation</th>
<th>Supported Escalation Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificate</td>
<td>.k5login</td>
</tr>
<tr>
<td>CyberArk</td>
<td>Cisco 'enable'</td>
</tr>
<tr>
<td>Kerberos</td>
<td>dzdo</td>
</tr>
<tr>
<td>password</td>
<td>pbrun</td>
</tr>
<tr>
<td>public key</td>
<td>su</td>
</tr>
<tr>
<td>Thycotic Secret Server</td>
<td>su+sudo</td>
</tr>
<tr>
<td></td>
<td>sudo</td>
</tr>
</tbody>
</table>

The tables below describe the additional credential options you must configure for privilege escalation.

**Note:** BeyondTrust's PowerBroker (pbrun) and Centrify's DirectAuthorize (dzdo) are proprietary root task delegation methods for Unix and Linux systems.

**Tip:** Scans run using su+sudo allow the user to scan with a non-privileged account and then switch to a user with sudo privileges on the remote host. This is important for locations where remote privileged login is prohibited.

**Note:** Scans run using sudo vs. the root user do not always return the same results because of the different environmental variables applied to the sudo user and other subtle differences. For more information, see: [https://www.sudo.ws/man/sudo.man.html](https://www.sudo.ws/man/sudo.man.html).

Privilege Escalation Options for Certificate, Kerberos, Password, and Public Key

<table>
<thead>
<tr>
<th>Option</th>
<th>Escalation Type</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable password</td>
<td>Cisco 'enable'</td>
<td>The password to run the 'enable' utility on a Cisco device.</td>
<td>yes</td>
</tr>
<tr>
<td>Escalation account</td>
<td>.k5login</td>
<td>The username for the account with</td>
<td>yes</td>
</tr>
<tr>
<td>Option</td>
<td>Escalation Type</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------</td>
<td>-------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>dzdo</td>
<td>elevated privileges.</td>
<td>The password for the account with elevated privileges.</td>
<td>yes</td>
</tr>
<tr>
<td>Location of dzdo (directory)</td>
<td>dzdo</td>
<td>The directory path for the dzdo command.</td>
<td>no</td>
</tr>
<tr>
<td>Location of pbrun (directory)</td>
<td>pbrun</td>
<td>The directory path for the pbrun command.</td>
<td>no</td>
</tr>
<tr>
<td>Location of su (directory)</td>
<td>su</td>
<td>The directory path for the su command.</td>
<td>no</td>
</tr>
<tr>
<td>Location of su and sudo (directory)</td>
<td>su+sudo</td>
<td>The directory path for the su and sudo commands.</td>
<td>no</td>
</tr>
<tr>
<td>Location sudo (directory)</td>
<td>sudo</td>
<td>The directory path for the sudo command.</td>
<td>no</td>
</tr>
<tr>
<td>SSH user password</td>
<td>pbrun</td>
<td>The password for the account with elevated privileges.</td>
<td>yes</td>
</tr>
<tr>
<td>su login</td>
<td>su</td>
<td>The username for the account with su privileges.</td>
<td>yes</td>
</tr>
<tr>
<td>su user</td>
<td>su+sudo</td>
<td>The username for the account with su privileges.</td>
<td>yes</td>
</tr>
<tr>
<td>sudo password</td>
<td>sudo</td>
<td>The password for the account with sudo privileges.</td>
<td>yes</td>
</tr>
<tr>
<td>sudo user</td>
<td>su+sudo</td>
<td>The username for the account with sudo privileges.</td>
<td>yes</td>
</tr>
<tr>
<td>CyberArk Account Details Name</td>
<td>.k5login Cisco 'enable' dzdo pbrun su su+sudo sudo</td>
<td>The name parameter for the Cyber-Ark account with elevated privileges.</td>
<td>yes</td>
</tr>
<tr>
<td>Escalation account</td>
<td>dzdo</td>
<td>The username for the account with elevated privileges.</td>
<td>yes</td>
</tr>
<tr>
<td>Location of dzdo (directory)</td>
<td>dzdo</td>
<td>The directory path for the dzdo command.</td>
<td>no</td>
</tr>
<tr>
<td>Location of pbrun (directory)</td>
<td>pbrun</td>
<td>The directory path for the pbrun command.</td>
<td>no</td>
</tr>
<tr>
<td>Location of su (directory)</td>
<td>su</td>
<td>The directory path for the su command.</td>
<td>no</td>
</tr>
<tr>
<td>Location of su and sudo (directory)</td>
<td>su+sudo</td>
<td>The directory path for the su and sudo commands.</td>
<td>no</td>
</tr>
<tr>
<td>Location sudo (directory)</td>
<td>sudo</td>
<td>The directory path for the sudo command.</td>
<td>no</td>
</tr>
<tr>
<td>su login</td>
<td>su</td>
<td>The username for the account with su privileges.</td>
<td>yes</td>
</tr>
<tr>
<td>su user</td>
<td>su+sudo</td>
<td>The username for the account with su privileges.</td>
<td>yes</td>
</tr>
<tr>
<td>sudo user</td>
<td>su+sudo sudo</td>
<td>The username for the account with sudo privileges.</td>
<td>yes</td>
</tr>
</tbody>
</table>

## Privilege Escalation Options for Thycotic Secret Server

<table>
<thead>
<tr>
<th>Option</th>
<th>Escalation Type</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Thycotic Escalation Account</strong></td>
<td><strong>.k5login</strong></td>
<td>The name parameter for the Thycotic account with elevated privileges.</td>
<td><strong>yes</strong></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------</td>
<td>-------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td></td>
<td>Cisco 'enable'</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>dzdo</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>pbrun</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>su</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>su+sudo</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>sudo</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Location of dzdo (directory)</strong></td>
<td>dzdo</td>
<td>The directory path for the dzdo command.</td>
<td><strong>no</strong></td>
</tr>
<tr>
<td><strong>Location of pbrun (directory)</strong></td>
<td>pbrun</td>
<td>The directory path for the pbrun command.</td>
<td><strong>no</strong></td>
</tr>
<tr>
<td><strong>Location of su (directory)</strong></td>
<td>su</td>
<td>The directory path for the su command.</td>
<td><strong>no</strong></td>
</tr>
<tr>
<td><strong>Location of su and sudo (directory)</strong></td>
<td>su+sudo</td>
<td>The directory path for the su and sudo commands.</td>
<td><strong>no</strong></td>
</tr>
<tr>
<td><strong>Location sudo (directory)</strong></td>
<td>sudo</td>
<td>The directory path for the sudo command.</td>
<td><strong>no</strong></td>
</tr>
<tr>
<td><strong>su user</strong></td>
<td>su+sudo</td>
<td>The username for the account with su privileges.</td>
<td><strong>yes</strong></td>
</tr>
</tbody>
</table>
Miscellaneous

Tenable.io supports the additional authentication methods described below.

**ADSI**

ADSI requires the domain controller information, domain, and domain admin and password.

ADSI allows Tenable.io to query an ActiveSync server to determine if any Android or iOS-based devices are connected. Using the credentials and server information, Tenable.io authenticates to the domain controller (not the Exchange server) to directly query it for device information. This feature does not require any ports be specified in the scan configuration. These settings are required for mobile device scanning.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Controller</td>
<td>(Required) Name of the domain controller for ActiveSync</td>
</tr>
<tr>
<td>Domain</td>
<td>(Required) Name of the Windows domain for ActiveSync</td>
</tr>
<tr>
<td>Domain Admin</td>
<td>(Required) Domain admin’s username</td>
</tr>
<tr>
<td>Domain Password</td>
<td>(Required) Domain admin’s password</td>
</tr>
</tbody>
</table>

Tenable.io supports obtaining the mobile information from Exchange Server 2010 and 2013 only; Tenable.io cannot retrieve information from Exchange Server 2007.

**F5**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>(Required) Username for a scanning account on the F5 target.</td>
</tr>
<tr>
<td>Password</td>
<td>(Required) Password associated with the scanning account.</td>
</tr>
<tr>
<td>Port</td>
<td>Port to use when connecting to the F5 target.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>When enabled, connect using secure communication (HTTPS). When disabled, connect using standard HTTP.</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>Verify that the SSL certificate is valid. If you are using a self-signed certificate, disable this setting.</td>
</tr>
</tbody>
</table>
### IBM iSeries

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>(Required) An iSeries username.</td>
</tr>
<tr>
<td>Password</td>
<td>(Required) An iSeries password.</td>
</tr>
</tbody>
</table>

### Netapp API

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>(Required) Username for an account on the Netapp system that has HTTPS access.</td>
</tr>
<tr>
<td>Password</td>
<td>(Required) Password associated with the account.</td>
</tr>
<tr>
<td>vFiler</td>
<td>If this setting is blank, the scan audits for all discovered Netapp virtual filers (vFilers) on target systems. To limit the audit to a single vFiler, type the name of the vFiler.</td>
</tr>
<tr>
<td>Port</td>
<td>Ports to scan on target systems. Type a comma-separated list of port numbers.</td>
</tr>
</tbody>
</table>

### OpenStack

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>(Required) Username for an account on the OpenStack deployment.</td>
</tr>
<tr>
<td>Password</td>
<td>(Required) Password associated with the account.</td>
</tr>
<tr>
<td>Tenant Name for Authentication</td>
<td>(Required) Name of the specific tenant the scan uses to authenticate. A tenant (also known as a project) is a group of resources that can be controlled by users in the tenant.</td>
</tr>
<tr>
<td>Port</td>
<td>(Required) Port that the scanner uses to connect to OpenStack.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>When enabled, connect using secure communication (HTTPS). When disabled, connect using standard HTTP.</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>Verify that the SSL certificate is valid. If you are using a self-signed cer-</td>
</tr>
</tbody>
</table>
Palo Alto Networks PAN-OS

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>(Required) The PAN-OS username.</td>
</tr>
<tr>
<td>Password</td>
<td>(Required) The Pan-OS password.</td>
</tr>
<tr>
<td>Port</td>
<td>(Required) The management port number.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Whether Tenable.io authenticates over an encrypted (HTTPS) or an unencrypted (HTTP) connection.</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>Verify that the SSL certificate is valid. If the target is using a self-signed certificate, disable this setting.</td>
</tr>
</tbody>
</table>

Red Hat Enterprise Virtualization (RHEV)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>(Required) Username to login to the RHEV server.</td>
</tr>
<tr>
<td>Password</td>
<td>(Required) Username to the password to login to the RHEV server.</td>
</tr>
<tr>
<td>Port</td>
<td>Port to connect to the RHEV server.</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>Verify that the SSL certificate for the RHEV server is valid.</td>
</tr>
</tbody>
</table>

VMware ESX SOAP API

Access to VMware servers is available through its native SOAP API. VMware ESX SOAP API allows you to access the ESX and ESXi servers via username and password. Additionally, you have the option of not enabling SSL certificate verification.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>(Required) Username to login to the ESXi server.</td>
</tr>
<tr>
<td>Password</td>
<td>(Required) Username to the password to login to the ESXi server.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Do not verify SSL Certificate</td>
<td>Do not verify that the SSL certificate for the ESXi server is valid.</td>
</tr>
</tbody>
</table>

**VMware vCenter SOAP API**

VMware vCenter SOAP API allows you to access vCenter. If available, the vCenter REST API is used to collect data in addition to the SOAP API.

**Note:** You must use a vCenter admin account with read and write permissions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Host</td>
<td>(Required) Name of the vCenter host.</td>
</tr>
<tr>
<td>vCenter Port</td>
<td>Port to access the vCenter host.</td>
</tr>
<tr>
<td>Username</td>
<td>(Required) Username to login to the vCenter server.</td>
</tr>
<tr>
<td>Password</td>
<td>(Required) Username to the password to login to the vCenter server.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Connect to the vCenter via SSL.</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>Verify that the SSL certificate for the ESXi server is valid.</td>
</tr>
</tbody>
</table>

**X.509**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client certificate</td>
<td>(Required) The client certificate.</td>
</tr>
<tr>
<td>Client key</td>
<td>(Required) The client private key.</td>
</tr>
<tr>
<td>Password for key</td>
<td>(Required) The passphrase for the key.</td>
</tr>
<tr>
<td>CA certificate to trust</td>
<td>(Required) The trusted Certificate Authority's (CA) digital certificate.</td>
</tr>
</tbody>
</table>
# Mobile

## AirWatch

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirWatch Environment API URL</td>
<td>-</td>
<td>The URL of the SOAP or REST API.</td>
<td>yes</td>
</tr>
<tr>
<td>Port</td>
<td>443</td>
<td>The port Tenable.io uses to authenticate with Airwatch.</td>
<td>yes</td>
</tr>
<tr>
<td>Username</td>
<td>-</td>
<td>The username to authenticate with Airwatch’s API.</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>-</td>
<td>The password to authenticate with Airwatch’s API.</td>
<td>yes</td>
</tr>
<tr>
<td>API Key</td>
<td>-</td>
<td>The API Key for the Airwatch REST API.</td>
<td>yes</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Enabled</td>
<td>Whether Tenable.io authenticates over an encrypted (HTTPS) or an unencrypted (HTTP) connection.</td>
<td>no</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>Enabled</td>
<td>Whether Tenable.io verifies if the SSL Certificate on the server is signed by a trusted CA.</td>
<td>no</td>
</tr>
</tbody>
</table>

## Apple Profile Manager

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>-</td>
<td>The server URL to authenticate with Apple Profile Manager.</td>
<td>yes</td>
</tr>
<tr>
<td>Port</td>
<td>443</td>
<td>The port Tenable.io uses to authenticate with Apple Profile Manager.</td>
<td>yes</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hostname</td>
<td>The server URL to authenticate with Blackberry UEM.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>The port to use to authenticate with Blackberry UEM.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tenant</td>
<td>The SRP ID in Blackberry UEM.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** To locate the SRP ID in Blackberry UEM:

1. In the Blackberry UEM top navigation bar, click the Help drop-down.
2. Click About Blackberry UEM.
   
   An information window appears containing the SRP ID.
3. Copy the SRP ID.
<table>
<thead>
<tr>
<th><strong>Domain</strong></th>
<th>The domain name for Blackberry UEM.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Username</strong></td>
<td>The username for the account you want Nessus to use to authenticate to Blackberry UEM.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password for the account you want Nessus to use to authenticate to Blackberry UEM.</td>
</tr>
<tr>
<td><strong>HTTPS</strong></td>
<td>When enabled, Tenable.io uses an encrypted connection to authenticate with Blackberry UEM.</td>
</tr>
<tr>
<td><strong>Verify SSL Certificate</strong></td>
<td>When enabled, Tenable.io verifies that the SSL Certificate on the server is signed by a trusted CA.</td>
</tr>
</tbody>
</table>

### Good MDM

<table>
<thead>
<tr>
<th><strong>Setting</strong></th>
<th><strong>Default Value</strong></th>
<th><strong>Description</strong></th>
<th><strong>Required</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server</strong></td>
<td>-</td>
<td>(Required) The server URL to authenticate with Good MDM.</td>
<td>yes</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>-</td>
<td>(Required) Set the port to use to authenticate with Good MDM.</td>
<td>yes</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>-</td>
<td>(Required) The domain name for Good MDM.</td>
<td>yes</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>-</td>
<td>(Required) The username to authenticate.</td>
<td>yes</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>-</td>
<td>(Required) The password to authenticate.</td>
<td>yes</td>
</tr>
<tr>
<td><strong>HTTPS</strong></td>
<td>Enabled</td>
<td>Whether Tenable.io authenticates over an encrypted (HTTPS) or an unencrypted (HTTP) connection.</td>
<td>no</td>
</tr>
<tr>
<td><strong>Verify SSL Certificate</strong></td>
<td>Enabled</td>
<td>Whether Tenable.io verifies if the SSL Certificate on the server is signed by a trusted CA.</td>
<td>no</td>
</tr>
</tbody>
</table>

### Intune
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant</td>
<td>The Microsoft Azure Directory (tenant) ID visible in your App registration.</td>
</tr>
</tbody>
</table>
| Client     | The Microsoft Azure Application (client) ID generated during your App regis-
|            | tration.                                                                    |
| Secret     | The secret key generated when you created your client secret key in Microsoft
|            | Azure.                                                                      |
| Username   | The username for the account you want Tenable.io to use to authenticate to   |
|            | Intune.                                                                     |
| Password   | The password for the account you want Tenable.io to use to authenticate to |
|            | Intune.                                                                     |

### MaaS360

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>-</td>
<td>The username to authenticate.</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>-</td>
<td>The password to authenticate.</td>
<td>yes</td>
</tr>
<tr>
<td>Root URL</td>
<td>-</td>
<td>The server URL to authenticate with MaaS360.</td>
<td>yes</td>
</tr>
<tr>
<td>Platform ID</td>
<td>-</td>
<td>The Platform ID provided for MaaS360.</td>
<td>yes</td>
</tr>
<tr>
<td>Billing ID</td>
<td>-</td>
<td>The Billing ID provided for MaaS360.</td>
<td>yes</td>
</tr>
<tr>
<td>App ID</td>
<td>-</td>
<td>The App ID provided for MaaS360.</td>
<td>yes</td>
</tr>
<tr>
<td>App Version</td>
<td>-</td>
<td>The App Version of MaaS360.</td>
<td>yes</td>
</tr>
<tr>
<td>App access key</td>
<td>-</td>
<td>The App Access Key provided for MaaS360.</td>
<td>yes</td>
</tr>
</tbody>
</table>

### MobileIron

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
</table>

---

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective
<table>
<thead>
<tr>
<th><strong>Value</strong></th>
<th><strong>Value</strong></th>
<th><strong>Value</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>VSP Admin Portal URL</td>
<td>-</td>
<td>The server URL Tenable.io uses to authenticate with the MobileIron Admin Portal.</td>
</tr>
<tr>
<td>VSP Admin Portal Port</td>
<td>443</td>
<td>The port Tenable.io uses to authenticate with the MobileIron Admin Portal.</td>
</tr>
<tr>
<td>Port</td>
<td>443</td>
<td>The port Tenable.io uses to authenticate with the MobileIron System Manager.</td>
</tr>
<tr>
<td>Username</td>
<td>-</td>
<td>The username to authenticate.</td>
</tr>
<tr>
<td>Password</td>
<td>-</td>
<td>The password to authenticate.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Enabled</td>
<td>Whether Tenable.io authenticates over an encrypted (HTTPS) or an unencrypted (HTTP) connection.</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>Enabled</td>
<td>Whether Tenable.io verifies if the SSL Certificate on the server is signed by a trusted CA.</td>
</tr>
</tbody>
</table>
Patch Management

Nessus Manager and Tenable.io can leverage credentials for the Red Hat Network Satellite, IBM BigFix, Dell KACE 1000, WSUS, and SCCM patch management systems to perform patch auditing on systems for which credentials may not be available to the Nessus scanner.

Options for these patch management systems can be found under **Credentials** in their respective drop-down menus: Symantec Altiris, IBM BigFix, Red Hat Satellite Server, Microsoft SCCM, Dell KACE K1000, and Microsoft WSUS.

IT administrators are expected to manage the patch monitoring software and install any agents required by the patch management system on their systems.

Scanning With Multiple Patch Managers

If multiple sets of credentials are supplied to Tenable.io for patch management tools, Tenable.io uses all of them. Available credentials are:

- Credentials supplied to directly authenticate to the target
- Dell KACE 1000
- IBM Tivoli Endpoint Manager (BigFix)
- Microsoft System Center Configuration Manager (SCCM)
- Microsoft Windows Server Update Services (WSUS)
- Red Hat Network Satellite Server
- Symantec Altiris

If credentials are provided for a host, as well as a patch management system, or multiple patch management systems, Tenable.io compares the findings between all methods and report on conflicts or provide a satisfied finding. Use the Patch Management Windows Auditing Conflicts plugins to highlight patch data differences between the host and a patch management system.

Dell KACE K1000

KACE K1000 is available from Dell to manage the distribution of updates and hotfixes for Linux, Windows, and Mac OS X systems. Tenable.io and SecurityCenter have the ability to query KACE K1000
to verify whether or not patches are installed on systems managed by KACE K1000 and display the patch information through the Tenable.io or SecurityCenter GUI.

**Note:** The Tenable.io KACE K1000 integration is only compatible up to KACE version 6.x.

- If the credential check sees a system but it is unable to authenticate against the system, it uses the data obtained from the patch management system to perform the check. If Tenable.io is able to connect to the target system, it performs checks on that system and ignore KACE K1000 output.
- The data returned to Tenable.io by KACE K1000 is only as current as the most recent data that the KACE K1000 has obtained from its managed hosts.

KACE K1000 scanning is performed using four Tenable.io plugins.

- `kace_k1000_get_computer_info.nbin` (Plugin ID 76867)
- `kace_k1000_get_missing_updates.nbin` (Plugin ID 76868)
- `kace_k1000_init_info.nbin` (Plugin ID 76866)
- `kace_k1000_report.nbin` (Plugin ID 76869)

Credentials for the Dell KACE K1000 system must be provided for K1000 scanning to work properly. Under the Credentials tab, select Patch Management and then Dell KACE K1000.

<table>
<thead>
<tr>
<th>Option</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>None</td>
<td>(Required) The KACE K1000 IP address or system name.</td>
</tr>
<tr>
<td>Database Port</td>
<td>3306</td>
<td>The port the K1000 database is running on (typically TCP 3306).</td>
</tr>
<tr>
<td>Organization Database Name</td>
<td>ORG1</td>
<td>The name of the organization component for the KACE K1000 database. This component begins with the letters ORG and ends with a number that corresponds with the K1000 database username.</td>
</tr>
<tr>
<td>Database Username</td>
<td>None</td>
<td>The username required to log into the K1000 database. R1 is the default if no user is defined. The username begins with</td>
</tr>
<tr>
<td>Option</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the letter R. This username ends in the same number that represents the number of the organization to scan.</td>
</tr>
<tr>
<td>Database Password</td>
<td>None</td>
<td>(Required) The password required to authenticate the K1000 Database Username.</td>
</tr>
</tbody>
</table>

IBM Tivoli Endpoint Manager (BigFix)

IBM BigFix is available to manage the distribution of updates and hotfixes for desktop systems. Tenable.io can query IBM BigFix to verify whether or not patches are installed on systems managed by IBM BigFix and display the patch information.

Tenable supports IBM BigFix 9.5 and later and 10.x and later.

- If the credential check sees a system but it is unable to authenticate against the system, it uses the data obtained from the patch management system to perform the check. If Tenable.io is able to connect to the target system, it performs checks on that system and ignores IBM BigFix output.
- The data returned to Tenable.io by IBM Big Fix is only as current as the most recent data that the IBM Big Fix server has obtained from its managed hosts.

IBM Big Fix scanning uses five Tenable plugins:

- Plugin 62558
- Plugin 62559
- Plugin 62561
- Plugin 62560
- Plugin 65703

You must provide credentials for the IBM Big Fix server for IBM Big Fix scanning to work properly.

<table>
<thead>
<tr>
<th>Option</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Reports Server</td>
<td>none</td>
<td>The name of IBM Big Fix Web Reports Server.</td>
</tr>
<tr>
<td>Option</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Web Reports Port</td>
<td>none</td>
<td>The port that the IBM BigFix Web Reports Server listens on.</td>
</tr>
<tr>
<td>Web Reports Username</td>
<td>none</td>
<td>The Web Reports administrative username.</td>
</tr>
<tr>
<td>Web Reports Password</td>
<td>none</td>
<td>The Web Reports administrative password.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Enabled</td>
<td>Shows if the Web Reports service is using SSL.</td>
</tr>
<tr>
<td>Verify SSL certificate</td>
<td>Enabled</td>
<td>Verifies that the SSL certificate is valid.</td>
</tr>
</tbody>
</table>

Package reporting is supported by RPM-based and Debian-based distributions that IBM BigFix officially supports. This includes Red Hat derivatives such as RHEL, CentOS, Scientific Linux, and Oracle Linux, as well as Debian and Ubuntu. Other distributions may also work, but unless IBM BigFix officially supports them, there is no support available.

For local check plugins to trigger, only RHEL, CentOS, Scientific Linux, Oracle Linux, Debian, Ubuntu, and Solaris are supported. Plugin 65703 must be enabled.

In order to use these auditing features, you must make changes to the IBM BigFix server. You must import a custom analysis into IBM BigFix so that detailed package information is retrieved and made available to Tenable.io.

From the HCL BigFix Console application, import the following .bes files.

**BES file:**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<BES xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="BES.xsd">
  <Analysis>
    <Title>Tenable</Title>
    <Description>This analysis provides SecurityCenter with the data it needs for vulnerability reporting.</Description>
    <Relevance>true</Relevance>
    <Source>Internal</Source>
    <SourceReleaseDate>2013-01-31</SourceReleaseDate>
    <MIMEField>
      <Name>x-fixlet-modification-time</Name>
      <Value>Thu, 13 May 2021 21:43:29 +0000</Value>
    </MIMEField>
  </Analysis>
</BES>
```
<Domain>BESC</Domain>

<Property Name="Packages - With Versions (Tenable)" ID="74"> <![CDATA[if (exists true whose (if true then repository) else false)) then unique values of (lpp_name of it & "|" & version of it as string & "|" & "fileset" tense of operating system) of files of products of object repository else if (exists true whose (if true then repository package) else false)) then unique values of (name of it & "|" & version of it as string & "|" & "deb" & "|" & it & ") & architecture of operating system) of packages whose (exists version of it) of debianpackages else if (true then (exists rpm) else false)) then unique values of (name of it & "|" & version of it as string & "|" & architecture of it & ") & architecture of operating system) of packages of rpm else if (exists true whose (exists ips image) else false)) then unique values of (full name of it & "|" & version of it as string & "|" & "architecture of operating system) of latest installed packages of ips image else if (exists true whose (if true then pkgdb) else false)) then unique values of(pkginst of it & "|" & version of it & "|" & pkg10) of pkginfos of pkg "unsupported">]]></Property>

<Property Name="Tenable AIX Technology Level" ID="76"> <![CDATA[current technology level of operating system]]></Property>

<Property Name="Tenable Solaris - Showrev -a" ID="77"> <![CDATA[if ((operating system as string as lowercase "SunOS 5.10" as lowercase) AND (exists file "/var/opt/BESClient/showrev_patches.b64") then lines of file "/var/opt/BESClient/showrev_patches.b64" else <unsupported>]]></Property>

</Analysis>
</BES>

## BES File:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<BES xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="BES.xsd">
  <Task>
    <Title>Tenable - Solaris 5.10 - showrev -a Capture</Title>
    <Description><![CDATA[&lt;enter a description of the task here;&gt;]]></Description>
    <GroupRelevance JoinByIntersection="False">
      <SearchComponentPropertyReference PropertyName="OS" Comparison="Contains">
        <SearchText>SunOS 5.10</SearchText>
        <Relevance>exists (operating system) whose (it as string as lowercase contains "SunOS 5.10" as lowercase)</Relevance>
      </SearchComponentPropertyReference>
    </GroupRelevance>
    <Category></Category>
    <Source>Internal</Source>
    <SourceID>/SourceID>
    <SourceReleaseDate>2021-05-12</SourceReleaseDate>
    <SourceSeverity>/SourceSeverity>
    <CVENames>/CVENames>
    <SANSID>/SANSID>
    <MIMEField>
      <Name>x-fixlet-modification-time</Name>
      <Value>Thu, 13 May 2021 21:50:58 +0000</Value>
    </MIMEField>
  </Task>
</BES>
```
Microsoft System Center Configuration Manager (SCCM)

Microsoft System Center Configuration Manager (SCCM) is available to manage large groups of Windows-based systems. Tenable.io has the ability to query the SCCM service to verify whether or not patches are installed on systems managed by SCCM and display the patch information through the scan results.

- If the credentialed check sees a system but it is unable to authenticate against the system, it uses the data obtained from the patch management system to perform the check. If Tenable.io is able to connect to the target system, it performs checks on that system and ignores SCCM output.

- The data returned by SCCM is only as current as the most recent data that the SCCM server has obtained from its managed hosts.

- Tenable.io connects to the server that is running the SCCM site (e.g., credentials must be valid for the SCCM service, so the selected user must have privileges to query all the data in the SCCM MMC). This server may also run the SQL database, or the database and the SCCM repository can be on separate servers. When leveraging this audit, configured sensors must connect to the SCCM server via WMI and HTTPS.

SCCM scanning is performed using four Tenable plugins.

- Patch Management: SCCM Server Settings (Plugin ID 57029)
- Patch Management: Missing updates from SCCM (Plugin ID 57030)
- Patch Management: SCCM Computer Info Initialization (Plugin ID 73636)
- Patch Management: SCCM Report (Plugin ID 58186)


You must provide the following SCCM system credentials for SCCM scanning to work properly.
<table>
<thead>
<tr>
<th>Credential</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server</strong></td>
<td>(Required) The SCCM IP address or system name.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>(Required) The domain the SCCM server is a part of.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>(Required) The SCCM user with privileges to query all data in the SCCM MMC, such as Read-only Analyst, Operations Administrator, or Full Administrator.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>(Required) The password for the SCCM user with privileges to query all data in the SCCM MMC.</td>
</tr>
</tbody>
</table>

**Microsoft Windows Server Update Services (WSUS)**

Windows Server Update Services (WSUS) is available from Microsoft to manage the distribution of updates and hotfixes for Microsoft products. Tenable.io and SecurityCenter have the ability to query WSUS to verify whether or not patches are installed on systems managed by WSUS and display the patch information through the Tenable.io or SecurityCenter GUI.

- If the credential check sees a system but it is unable to authenticate against the system, it uses the data obtained from the patch management system to perform the check. If Tenable.io is able to connect to the target system, it performs checks on that system and ignores WSUS output.
- The data returned to Tenable.io by WSUS is only as current as the most recent data that the WSUS server has obtained from its managed hosts.

WSUS scanning is performed using three Tenable.io plugins.

- **Patch Management: WSUS Server Settings** (Plugin ID 57031)
- **Patch Management: Missing updates from WSUS** (Plugin ID 57032)
- **Patch Management: WSUS Report** (Plugin ID 58133)

Credentials for the WSUS system must be provided for WSUS scanning to work properly. Under the Credentials tab, select Patch Management and then Microsoft WSUS.
<table>
<thead>
<tr>
<th>Credential</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>None</td>
<td>(Required) The WSUS IP address or system name.</td>
</tr>
<tr>
<td>Port</td>
<td>8530</td>
<td>The port WSUS is running on.</td>
</tr>
<tr>
<td>Username</td>
<td>None</td>
<td>(Required) The WSUS admin username.</td>
</tr>
<tr>
<td>Password</td>
<td>None</td>
<td>(Required) The WSUS admin password.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Enabled</td>
<td>Shows if the WSUS service is using SSL.</td>
</tr>
<tr>
<td>Verify SSL certificate</td>
<td>Enabled</td>
<td>Verifies that the SSL certificate is valid.</td>
</tr>
</tbody>
</table>

**Red Hat Satellite 5 Server**

Red Hat Satellite is a systems management platform for Linux-based systems. Tenable.io has the ability to query Satellite to verify whether or not patches are installed on systems managed by Satellite and display the patch information.

Although not supported by Tenable, the RHN Satellite plugin also works with Spacewalk Server, the Open Source Upstream Version of Red Hat Satellite. Spacewalk has the capability of managing distributions based on Red Hat (RHEL, CentOS, Fedora) and SUSE. Tenable supports the Satellite server for Red Hat Enterprise Linux.

- If the credential check sees a system, but it is unable to authenticate against the system, it uses the data obtained from the patch management system to perform the check. If Tenable.io is able to connect to the target system, it performs checks on that system and ignores RHN Satellite output.
- The data returned to Tenable.io by RHN Satellite is only as current as the most recent data that the Satellite server has obtained from its managed hosts.

If the RHN Satellite server is version 5, scanning is performed using the following Tenable.io plugins:

- Patch Management: Patch Schedule From Red Hat Satellite Server (Plugin ID 84236)
- Patch Management: Red Hat Satellite Server Get Installed Packages (Plugin ID 84235)
- Patch Management: Red Hat Satellite Server Get Managed Servers (Plugin ID 84234)
Patch Management: Red Hat Satellite Server Get System Information (Plugin ID 84237)

Patch Management: Red Hat Satellite Server Settings (Plugin ID 84238)

<table>
<thead>
<tr>
<th>Credential</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Satellite server</td>
<td>None</td>
<td>(Required) The RHN Satellite IP address or system name.</td>
</tr>
<tr>
<td>Port</td>
<td>443</td>
<td>(Required) The port Satellite is running on (typically TCP 80 or 443).</td>
</tr>
<tr>
<td>Username</td>
<td>None</td>
<td>(Required) The Red Hat Satellite username.</td>
</tr>
<tr>
<td>Password</td>
<td>None</td>
<td>(Required) The Red Hat Satellite password.</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>Enabled</td>
<td>Verifies that the SSL certificate is valid.</td>
</tr>
</tbody>
</table>

Red Hat Satellite 6 Server

Red Hat Satellite is a systems management platform for Linux-based systems. Tenable.io has the ability to query Satellite to verify whether or not patches are installed on systems managed by Satellite and display the patch information. For more information, see the description of the Red Hat Satellite 5 Server settings.

If the RHN Satellite server is version 6, scanning is performed using the same plugins as version 5, plus three additional Tenable.io plugins:

- Patch Management: Red Hat Satellite Server Get Installed Packages (Plugin ID 84231)
- Patch Management: Red Hat Satellite 6 Settings (Plugin ID 84232)
- Patch Management: Red Hat Satellite 6 Report (Plugin ID 84233)

<table>
<thead>
<tr>
<th>Credential</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Satellite server</td>
<td>None</td>
<td>(Required) The RHN Satellite IP address or system name.</td>
</tr>
<tr>
<td>Port</td>
<td>443</td>
<td>The port Satellite is running on (typically TCP 80 or 443).</td>
</tr>
<tr>
<td>Credential</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Username</td>
<td>None</td>
<td>(Required) The Red Hat Satellite username.</td>
</tr>
<tr>
<td>Password</td>
<td>None</td>
<td>(Required) The Red Hat Satellite password.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Enabled</td>
<td>Determines whether Tenable.io sends the credentials over a secure HTTP connection.</td>
</tr>
<tr>
<td>Verify SSL</td>
<td>Enabled</td>
<td>Verifies that the SSL certificate is valid.</td>
</tr>
<tr>
<td>Certificate</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Symantec Altiris

Altiris is available from Symantec to manage the distribution of updates and hotfixes for Linux, Windows, and Mac OS X systems. Tenable.io and SecurityCenter have the ability to use the Altiris API to verify whether or not patches are installed on systems managed by Altiris and display the patch information through the Tenable.io or SecurityCenter GUI.

- If the credential check sees a system but it is unable to authenticate against the system, it uses the data obtained from the patch management system to perform the check. If Tenable.io is able to connect to the target system, it performs checks on that system and ignores Altiris output.
- The data returned to Tenable.io by Altiris is only as current as the most recent data that the Altiris has obtained from its managed hosts.
- Tenable.io connects to the Microsoft SQL server that is running on the Altiris host (e.g., credentials must be valid for the MSSQL database, meaning a database account with the privileges to query all the data in the Altiris MSSQL database). The database server may be run on a separate host from the Altiris deployment. When leveraging this audit, Tenable.io must connect to the MSSQL database, not the Altiris server if the two are on separate boxes.

Altiris scanning is performed using four Tenable.io plugins.

- symantec_altiris_get_computer_info.nbin (Plugin ID 78013)
- symantec_altiris_get_missing_updates.nbin (Plugin ID 78012)
- symantec_altiris_init_info.nbin (Plugin ID 78011)
- symantec.altiris_report.nbin (Plugin ID 78014)

Credentials for the Altiris Microsoft SQL (MSSQL) database must be provided for Altiris scanning to work properly. Under the Credentials tab, select Patch Management and then Symantec Altiris.

<table>
<thead>
<tr>
<th>Credential</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>None</td>
<td>(Required) Altiris IP address or system name.</td>
</tr>
<tr>
<td>Database Port</td>
<td>5690</td>
<td>The port the Altiris database is running on (Typically TCP 5690).</td>
</tr>
<tr>
<td>Database Name</td>
<td>Symantec_CMDB</td>
<td>The name of the MSSQL database that manages Altiris patch information.</td>
</tr>
<tr>
<td>Database Username</td>
<td>None</td>
<td>(Required) The username required to log into the Altiris MSSQL database.</td>
</tr>
<tr>
<td>Database Password</td>
<td>None</td>
<td>(Required) The password required to authenticate the Altiris MSSQL database.</td>
</tr>
<tr>
<td>Use Windows Authentication</td>
<td>Disabled</td>
<td>Denotes whether or not to use NTLMSSP for compatibility with older Windows Servers, otherwise it uses Kerberos.</td>
</tr>
</tbody>
</table>

To ensure Tenable.io can properly utilize Altiris to pull patch management information, it must be configured to do so.
Plaintext Authentication

Caution: Using plaintext credentials is not recommended. Use encrypted authentication methods when possible.

If a secure method of performing credentialed checks is not available, you can configure Tenable.io to perform checks over unsecure protocols using the Plaintext Authentication settings.

FTP

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>-</td>
<td>Login user’s name.</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>-</td>
<td>Password of the user specified.</td>
<td>yes</td>
</tr>
</tbody>
</table>

HTTP

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication method</td>
<td>HTTP Login Form</td>
<td>The authentication method. Supported values are:</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Automatic authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Basic/Digest authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HTTP login form – Controls where authenticated testing of a custom web-based application begins.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HTTP cookies import – Facilitates web application testing by using cookies imported from another piece of software (e.g., web browser, web proxy, etc.) when attempting to access a web application.</td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td>Default</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------</td>
<td>--------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><strong>Method: Automatic Authentication</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>-</td>
<td>Login user's name.</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>-</td>
<td>Password of the user specified.</td>
<td>yes</td>
</tr>
<tr>
<td><strong>Method: Basic/Digest authentication</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>-</td>
<td>Login user's name.</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>-</td>
<td>Password of the user specified.</td>
<td>yes</td>
</tr>
<tr>
<td><strong>Method: HTTP login form</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>-</td>
<td>Login user's name.</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>-</td>
<td>Password of the user specified.</td>
<td>yes</td>
</tr>
<tr>
<td>Login page</td>
<td>-</td>
<td>The absolute path to the login page of the application, e.g., /login.html.</td>
<td>yes</td>
</tr>
<tr>
<td>Login submission page</td>
<td>-</td>
<td>The action parameter for the form method. For example, the login form for &lt;form method=&quot;POST&quot; name=&quot;auth_form&quot; action=&quot;/login.php&quot;&gt; would be /login.php.</td>
<td>yes</td>
</tr>
<tr>
<td>Login parameters</td>
<td>-</td>
<td>Specify the authentication parameters (e.g., login-n=%USER%&amp;password=%PASS%). If the keywords %USER% and %PASS% are used, the keywords will be substituted with values supplied on the Login configurations drop-down menu. This field can be used to provide more than two parameters if required (e.g., a group name or some other piece of information</td>
<td>yes</td>
</tr>
<tr>
<td>Setting</td>
<td>Default</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Check authentication on page</td>
<td>-</td>
<td>The absolute path of a protected web page that requires authentication, to better assist Tenable.io in determining authentication status, e.g., /admin.html.</td>
<td>yes</td>
</tr>
<tr>
<td>Regex to verify successful authentication</td>
<td>-</td>
<td>A regex pattern to look for on the login page. Simply receiving a 200 response code is not always sufficient to determine session state. Tenable.io can attempt to match a given string such as Authentication successful!</td>
<td>yes</td>
</tr>
<tr>
<td>Method: HTTP cookies import</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cookies file</td>
<td>-</td>
<td>Upload a cookie file. The file must be in Netscape format.</td>
<td>yes</td>
</tr>
<tr>
<td>All methods: Scan-wide Credential Type Settings</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login method</td>
<td>POST</td>
<td>Specify if the login action is performed via a GET or POST request.</td>
<td>yes</td>
</tr>
<tr>
<td>Re-authenticate delay (seconds)</td>
<td>0</td>
<td>The time delay between authentication attempts. Setting a time delay is useful to avoid triggering brute force lockout mechanisms.</td>
<td>yes</td>
</tr>
<tr>
<td>Follow 30x redirects (# of levels)</td>
<td>0</td>
<td>If a 30x redirect code is received from a web server, this setting directs Tenable.io to follow the link provided or not.</td>
<td>yes</td>
</tr>
</tbody>
</table>
| Invert authenticated regex                  | Disabled| A regex pattern to look for on the login page, that if found, tells Tenable.io that | no
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Value</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Value</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Value</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default Value</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Required</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IMAP**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>-</td>
<td>Login user's name.</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>-</td>
<td>Password of the user specified.</td>
<td>yes</td>
</tr>
</tbody>
</table>

**IPMI**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>-</td>
<td>Login user's name.</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>-</td>
<td>Password of the user specified.</td>
<td>yes</td>
</tr>
</tbody>
</table>

**NNTP**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>-</td>
<td>Login user's name.</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>-</td>
<td>Password of the user specified.</td>
<td>yes</td>
</tr>
</tbody>
</table>

**POP2**
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>-</td>
<td>Login user’s name.</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>-</td>
<td>Password of the user specified.</td>
<td>yes</td>
</tr>
</tbody>
</table>

### POP3

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>-</td>
<td>Login user’s name.</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>-</td>
<td>Password of the user specified.</td>
<td>yes</td>
</tr>
</tbody>
</table>

### SNMPv1/v2c

SNMPv1/v2c configuration allows you to use community strings for authentication to network devices. You can configure up to four SNMP community strings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community string</td>
<td>public</td>
<td>The community string Tenable.io uses to authenticate on the host device.</td>
<td>yes</td>
</tr>
</tbody>
</table>

**Scan-wide Credential Type Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP Port</td>
<td>161</td>
<td>Ports where Tenable.io attempts to authenticate on the host device.</td>
<td>no</td>
</tr>
<tr>
<td>Additional UDP port #1</td>
<td>161</td>
<td></td>
<td>no</td>
</tr>
<tr>
<td>Additional UDP port #2</td>
<td>161</td>
<td></td>
<td>no</td>
</tr>
<tr>
<td>Additional UDP port #3</td>
<td>161</td>
<td></td>
<td>no</td>
</tr>
</tbody>
</table>

### telnet/rsh/rexec

Tenable.io performs patch auditing on non-Windows targets only.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>-</td>
<td>Login user’s name.</td>
<td>yes</td>
</tr>
<tr>
<td>Password</td>
<td>-</td>
<td>Password of the user specified.</td>
<td>yes</td>
</tr>
</tbody>
</table>

**Scan-wide Credential Type Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform patch audits over telnet</td>
<td>Disabled</td>
<td>Tenable.io uses telnet to connect to the host device for patch audits.</td>
<td>no</td>
</tr>
<tr>
<td>Perform patch audits over rsh</td>
<td>Disabled</td>
<td>Tenable.io uses rsh to connect to the host device for patch audits.</td>
<td>no</td>
</tr>
<tr>
<td>Perform patch audits over rexec</td>
<td>Disabled</td>
<td>Tenable.io uses rexec to connect to the host device for patch audits.</td>
<td>no</td>
</tr>
</tbody>
</table>
Credentials in WAS Scans

Note: The topics in this section describe credentials in the new interface only. If you activate the new interface, you can view a snapshot of historical credentials that you configured in the classic interface, but you cannot modify those credentials.

For information about credentials in the classic interface, see WAS Credentials (Classic Interface).

In web application scans, you can configure credentials settings that allow Tenable.io Web Application Scanning to perform an authenticated scan on a web application. Credentialed scans can perform a wider variety of checks than non-credentialed scans, which can result in more accurate scan results.

Scans in Tenable.io Web Application Scanning use managed credentials. Managed credentials allow you to store credential settings centrally in a credential manager. You can then add those credential settings to multiple scan configurations instead of configuring credential settings for each individual scan.

Web application scans support credentials in the following authentication types:

- HTTP Server Authentication
- WAS Scan Web Application Authentication

Tip: If want to scan an API with the API scan template, and your API requires keys or a token for authentication, you can add the expected custom headers in the Advanced settings in the HTTP Settings section.

You can configure credentials settings in web application scans using the following methods:

<table>
<thead>
<tr>
<th>Credentials Category</th>
<th>Authentication Type</th>
<th>Configuration Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Server Authentication</td>
<td>-</td>
<td>Use the Tenable.io Web Application Scanning user interface to manually configure credentials settings in scans.</td>
</tr>
<tr>
<td>Web Application Authentication</td>
<td>Login Form</td>
<td>Use the Tenable.io Web Application Scanning user interface to <a href="#">manually configure credentials settings in scans</a>.</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cookie</td>
<td></td>
<td>Do one of the following:</td>
</tr>
</tbody>
</table>
| Selenium                      |            | - Use the Selenium Integrated Development Environment (IDE) extension in Chrome to record credentials, then [manually add the credentials to scans](#) via the Tenable.io Web Application Scanning user interface.  
  **Note:** For information about the Selenium IDE extension in Chrome, see the Google Chrome documentation. |
|                               |            | - Use the Tenable.io Web Application Scanning Chrome Extension to [record credentials and automatically add the credentials to your scan configurations](#).  
  **Tip:** For information about Selenium scripts you can use with Tenable.io Web Application Scanning, see [WAS Selenium Commands](#). |
Configure Credentials Settings in a WAS Scan

**Required Additional License:** Tenable.io Web Application Scanning

**Required Tenable.io Web Application Scanning User Role:** Scan Manager or Administrator

Before you begin:

- (Cookie authentication) Determine the cookie authentication credentials for the web application you want to scan.
- (Selenium authentication) In the [Chrome Web Store](https://chrome.google.com/webstore/detail/selenium-ide/lkkpomikcicmijoojmjkmkibddhjpnob), download the Selenium IDE extension, do one of the following:
  - To configure credentials using the Selenium IDE extension, download the Selenium IDE extension.
  - To configure credentials via the WAS Chrome Extension, download the Tenable.io Web Application Scanning Chrome Extension.

To configure credentials settings in a web application scan:

1. **Create** or **edit** a scan.
2. Click **Credentials**.
   
   The credentials details appear.
3. Next to **Add Credentials**, click the + button.
   
   The Select Credential Type plane appears.
4. Do one of the following:
   
   - Add existing credentials.
     
     The Managed Credentials section of the Select Credential Type plane contains any credentials where you have Can Use or Can Edit permissions.
a. (Optional) Search for a managed credential in the list by typing your search criteria in the text box and clicking the search button.

b. In the Managed Credentials section, click each managed credential you want to add.

The Select Credential Type plane remains open.

c. To close the Select Credential Type plane, click the close button in the upper-right corner of the plane.

• Create new credentials.

  a. In the Web Application Authentication section, click the credentials type you want to create:

     • HTTP Server Application

     • Web Application Authentication

     The settings plane for that credential type appears.

  b. In the first text box, type a name for the credentials.

  c. (Optional) In the second text box, type a description for the credentials.

  d. Configure the settings for the credentials type:

     • HTTP Server Application

     • Web Application Authentication

5. Add user permissions.

6. Click Save to save the credentials changes.

   Tenable.io Web Application Scanning closes the settings plane and adds the credentials to the credentials table for the scan.

   If you created new credentials, Tenable.io Web Application Scanning adds the credentials to the credential manager.

7. Click Save to save the scan changes.
Configure Selenium Credentials Settings Automatically

**Required Additional License:** Tenable.io Web Application Scanning

You can use the Tenable.io Web Application Scanning Chrome Extension to record Selenium credentials and add those credentials automatically to new or existing scans.

**Note:** The Tenable.io Web Application Scanning Chrome Extension updates only Selenium credentials settings in web application scans. You must configure the other scan options via the Tenable.io Web Application Scanning Chrome Extension interface.

Before you begin:

- Download the Tenable.io Web Application Scanning Chrome Extension from the [Chrome Web Store](https://chrome.google.com/webstore/detail/tenable-webapp-scanning-extension/bcfgadjmniiklbhgpdpkmkcmoofajgfl).
- Log in to Tenable.io, as described in [Log in to Tenable.io](https).

To record selenium credentials via the Tenable.io Web Application Scanning Chrome Extension:

1. In the upper-right corner of your browser, click the Tenable.io logo.

   The Tenable.io Web Application Scanning Chrome Extension Create a Scan window appears.

2. Do one of the following:

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
</table>
   | Record and add Selenium credentials to an existing scan | Click **Add to Existing Scan**.  
   |                                            | The **Add to Existing Scan** window appears, displaying a list of your existing scans.  
   |                                            | In the search box, type the name of the scan you want to add Selenium credentials to.  
   |                                            | Click the **button.** |
The Tenable.io Web Application Scanning Chrome Extension filters the list by the name you typed.

- Click the scan you want to add Selenium credentials to.

| Record and add Selenium credentials to a new scan | Click **Create New Scan**.  
The **New Scan** window appears.  
- In the **Name** box, type a name for your scan.  
- In the **URL** box, type the target in URL format for the web application you want to scan. |

3. Click **Next**.

   The extension opens to the link you provided as your scan target.

4. Click **Record**.

   The Tenable.io Web Application Scanning Chrome Extension begins recording your session.

   A **Tenable.io is recording** message appears.

5. Perform the log in sequence you use to authenticate into your web application.

6. After you successfully authenticate into the system, highlight a section of text on the web page that appears only upon successful authentication (for example, **Welcome, [your username]!**).

7. In the lower-right corner, click **Done**.

8. (Optional) To play back your recorded login sequence, click **Play**.

9. After you have successfully recorded your authentication login sequence, click **Save**.

   Tenable.io Web Application Scanning Chrome Extension saves and imports your credentials to the scan.

What to do next:
If you used the Tenable.io Web Application Scanning Chrome Extension to create a new scan, you must configure the other scan options in the Tenable.io Web Application Scanning Chrome Extension interface.
## WAS Selenium Commands

Selenium commands in Tenable.io Web Application Scanning are used to record authentication and crawling scripts so that users can tell the scanner exactly what to do in certain scenarios. You can run these commands in the Selenium IDE Extension or in the Tenable.io Web Application Scanning Chrome Extension, both available for download in the [Chrome Web Store](https://chrome.google.com/webstore/detail/tenable-sele-web-app-scan/aekgoppkmgpocdlpmhmmhjdpkognlfek).

Support for Selenium commands in Tenable.io Web Application Scanning is detailed below:

<table>
<thead>
<tr>
<th>Commands Supported</th>
<th>Commands Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>• addSelection</td>
<td>• close</td>
</tr>
<tr>
<td>• answerOnNextPrompt</td>
<td>• debugger</td>
</tr>
<tr>
<td>• assert</td>
<td>• do</td>
</tr>
<tr>
<td>• assertAlert</td>
<td>• else</td>
</tr>
<tr>
<td>• assertChecked</td>
<td>• else if</td>
</tr>
<tr>
<td>• assertConfirmation</td>
<td>• end</td>
</tr>
<tr>
<td>• assertEditable</td>
<td>• execute async script</td>
</tr>
<tr>
<td>• assertElementNotPresent</td>
<td>• execute script</td>
</tr>
<tr>
<td>• assertElementPresent</td>
<td>• for each</td>
</tr>
<tr>
<td>• assertNotChecked</td>
<td>• if</td>
</tr>
<tr>
<td>• assertNotEditable</td>
<td>• repeat if</td>
</tr>
<tr>
<td>• assertNotSelectedValue</td>
<td>• run</td>
</tr>
<tr>
<td>• assertNotText</td>
<td>• select window</td>
</tr>
<tr>
<td>• assertPrompt</td>
<td>• store</td>
</tr>
<tr>
<td>• assertSelectedLabel</td>
<td>• store attribute</td>
</tr>
<tr>
<td>• assertSelectedValue</td>
<td>• store json</td>
</tr>
<tr>
<td>• assertText</td>
<td>• store text</td>
</tr>
</tbody>
</table>

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
<table>
<thead>
<tr>
<th>Actions</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>assertTitle</td>
<td>store title</td>
</tr>
<tr>
<td>assertValue</td>
<td>store value</td>
</tr>
<tr>
<td>check</td>
<td>store window handle</td>
</tr>
<tr>
<td>chooseCancelOnNextConfirmation</td>
<td>store xpath count</td>
</tr>
<tr>
<td>chooseCancelOnNextPrompt</td>
<td>times</td>
</tr>
<tr>
<td>chooseOkOnNextConfirmation</td>
<td>while</td>
</tr>
<tr>
<td>click</td>
<td></td>
</tr>
<tr>
<td>clickAt</td>
<td></td>
</tr>
<tr>
<td>doubleClick</td>
<td></td>
</tr>
<tr>
<td>doubleClickAt</td>
<td></td>
</tr>
<tr>
<td>echo</td>
<td></td>
</tr>
<tr>
<td>editContent</td>
<td></td>
</tr>
<tr>
<td>mouseDown</td>
<td></td>
</tr>
<tr>
<td>mouseDownAt</td>
<td></td>
</tr>
<tr>
<td>mouseMoveAt</td>
<td></td>
</tr>
<tr>
<td>mouseOut</td>
<td></td>
</tr>
<tr>
<td>mouseOver</td>
<td></td>
</tr>
<tr>
<td>mouseUp</td>
<td></td>
</tr>
<tr>
<td>mouseUpAt</td>
<td></td>
</tr>
<tr>
<td>open</td>
<td></td>
</tr>
<tr>
<td>pause</td>
<td></td>
</tr>
<tr>
<td>removeSelection</td>
<td></td>
</tr>
<tr>
<td>runScript</td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>select</td>
</tr>
<tr>
<td>selectFrame</td>
</tr>
<tr>
<td>sendKeys</td>
</tr>
</tbody>
</table>

**Note:** In addition to arbitrary text, the `sendKeys` command only supports the following escape sequences:

- `${KEY_ENTER}`
- `${KEY_DELETE}`
- `${KEY_BACKSPACE}`

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>setSpeed</td>
</tr>
<tr>
<td>setWindowSize</td>
</tr>
<tr>
<td>submit</td>
</tr>
<tr>
<td>type</td>
</tr>
<tr>
<td>uncheck</td>
</tr>
<tr>
<td>verify</td>
</tr>
<tr>
<td>verifyChecked</td>
</tr>
<tr>
<td>verifyEditable</td>
</tr>
<tr>
<td>verifyElementNotPresent</td>
</tr>
<tr>
<td>verifyElementPresent</td>
</tr>
<tr>
<td>verifyNotChecked</td>
</tr>
<tr>
<td>verifyNotEditable</td>
</tr>
<tr>
<td>verifyNotSelectedValue</td>
</tr>
<tr>
<td>verifyNotText</td>
</tr>
<tr>
<td>verifySelectedLabel</td>
</tr>
<tr>
<td>verifySelectedValue</td>
</tr>
</tbody>
</table>
- verifyText
- verifyTitle
- verifyValue
- waitForElementEditable
- waitForElementNotEditable
- waitForElementNotPresent
- waitForElementNotVisible
- waitForElementPresent
- waitForElementVisible
- webdriverAnswerOnNextPrompt
- webdriverAnswerOnVisiblePrompt
- webdriverChooseCancelOnNextConfirmation
- webdriverChooseCancelOnNextPrompt
- webdriverChooseCancelOnVisibleConfirmation
- webdriverChooseCancelOnVisiblePrompt
- webdriverChooseOkOnNextConfirmation
- webdriverChooseOkOnVisibleConfirmation
# HTTP Server Authentication Settings in WAS Scans

In a web application scan, you can configure the following settings for HTTP server-based authentication credentials.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Type the username Tenable.io Web Application Scanning uses to authenticate to the HTTP-based server.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password Tenable.io Web Application Scanning uses to authenticate to the HTTP-based server.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>In the drop-down list, select one of the following authentication types:</td>
</tr>
<tr>
<td></td>
<td>• Basic/Digest</td>
</tr>
<tr>
<td></td>
<td>• NTLM</td>
</tr>
</tbody>
</table>
WAS Scan Web Application Authentication

In a web application scan, you can configure one of the following types of Web Application Authentication credentials:

- **Login Form Authentication**
- **Cookie Authentication**
- **Selenium Authentication**

## Login Form Authentication

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Method</td>
<td>In the drop-down box, select <strong>Login Form</strong>.</td>
</tr>
<tr>
<td>Login Page</td>
<td>Type the URL of the login page for the web application you want to scan.</td>
</tr>
<tr>
<td>Credentials</td>
<td>Do the following:</td>
</tr>
<tr>
<td></td>
<td>a. In the first <strong>Credentials</strong> text box, type a username that Tenable.io Web Application Scanning uses to log in to the web application.</td>
</tr>
<tr>
<td></td>
<td>b. In the second <strong>Credentials</strong> text box, type the password that Tenable.io Web Application Scanning uses to log in to the web application.</td>
</tr>
<tr>
<td></td>
<td>c. (Optional) Add alternate credentials by clicking the <strong>+</strong> button.</td>
</tr>
<tr>
<td>Pattern to Verify</td>
<td>Type a word, phrase, or regular expression that appears on the website only if the authentication is successful (for example, <strong>Welcome, your username</strong>). Note that leading slashes will be escaped and <code>.*</code> is not required at the beginning or end of the pattern.</td>
</tr>
<tr>
<td>Successful Auth</td>
<td></td>
</tr>
<tr>
<td>Page to Verify Action</td>
<td>Type the URL that Tenable.io Web Application Scanning can continually</td>
</tr>
<tr>
<td>Option</td>
<td>Action</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>In the drop-down box, select <strong>Cookie Authentication</strong>.</td>
</tr>
<tr>
<td>Session Cookies</td>
<td>Do the following:</td>
</tr>
<tr>
<td></td>
<td>a. In the first text box, type the name of the cookie authentication credentials.</td>
</tr>
<tr>
<td></td>
<td>b. In the second box, type the value of the cookie authentication credentials.</td>
</tr>
<tr>
<td>Pattern to Verify Successful Auth</td>
<td>Type a word, phrase, or regular expression that appears on the website only if the authentication is successful (for example, <strong>Welcome, your username</strong>). Note that leading slashes will be escaped and * is not required at the beginning or end of the pattern.</td>
</tr>
<tr>
<td>Page to Verify Active Session</td>
<td>Type the URL that Tenable.io Web Application Scanning can continually access to validate the authenticated session.</td>
</tr>
<tr>
<td>Pattern to Verify Active Session</td>
<td>Type a word, phrase, or regular expression that appears on the website only if the session is still active (for example, <strong>Hello, your username</strong>). Note that leading slashes will be escaped and * is not required at the beginning or end of the pattern.</td>
</tr>
</tbody>
</table>

**Cookie Authentication**

**Selenium Authentication**
<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Method</td>
<td>Select <strong>Selenium Authentication</strong>.</td>
</tr>
<tr>
<td>Selenium Script (.side)</td>
<td>Do the following:</td>
</tr>
<tr>
<td></td>
<td>a. In the Selenium IDE extension, record your authentication credentials in the Selenium IDE extension.</td>
</tr>
<tr>
<td></td>
<td>b. Click <strong>Add File</strong>. The file explorer for your operating system appears.</td>
</tr>
<tr>
<td></td>
<td>c. Navigate to and select your Selenium credentials .side file. Tenable.io Web Application Scanning imports the credentials file.</td>
</tr>
<tr>
<td>Pattern to Verify Successful Auth</td>
<td>Type a word, phrase, or regular expression that appears on the website only if the authentication is successful (for example, <em>Welcome, your username!</em>). Note that leading slashes will be escaped and .* is not required at the beginning or end of the pattern.</td>
</tr>
<tr>
<td>Page to Verify Active Session</td>
<td>Type the URL that Tenable.io Web Application Scanning can continually access to validate the authenticated session.</td>
</tr>
<tr>
<td>Pattern to Verify Active Session</td>
<td>Type a word, phrase, or regular expression that appears on the website only if the session is still active (for example, <em>Hello, your username!</em>). Note that leading slashes will be escaped and .* is not required at the beginning or end of the pattern.</td>
</tr>
</tbody>
</table>
Compliance in Vulnerability Management Scans

**Note:** If a scan is based on a user-defined template, you cannot configure Compliance settings in the scan. You can only modify these settings in the related user-defined template.

Tenable.io can perform vulnerability scans of network services as well as log in to servers to discover any missing patches.

However, a lack of vulnerabilities does not mean the servers are configured correctly or are "compliant" with a particular standard.

You can use Tenable.io to perform vulnerability scans and compliance audits to obtain all of this data at one time. If you know how a server is configured, how it is patched, and what vulnerabilities are present, you can determine measures to mitigate risk.

At a higher level, if this information is aggregated for an entire network or asset class, security and risk can be analyzed globally. This allows auditors and network managers to spot trends in non-compliant systems and adjust controls to fix these on a larger scale.

When configuring a scan or policy, you can include one or more compliance checks, also known as audits. Each compliance check requires specific **credentials**.

Some compliance checks are preconfigured by Tenable, but you can also create and upload custom audits.

For more information on compliance checks and creating custom audits, see the Compliance Checks Reference.

<table>
<thead>
<tr>
<th>Compliance Check</th>
<th>Required Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adtran AOS</td>
<td>SSH</td>
</tr>
<tr>
<td>Alcatel TiMOS</td>
<td>SSH</td>
</tr>
<tr>
<td>Amazon AWS</td>
<td>Amazon AWS</td>
</tr>
<tr>
<td>Arista EOS</td>
<td>SSH</td>
</tr>
<tr>
<td>Blue Coat ProxySG</td>
<td>SSH</td>
</tr>
<tr>
<td>Brocade FabricOS</td>
<td>SSH</td>
</tr>
<tr>
<td>Product</td>
<td>Method</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Check Point GAiA</td>
<td>SSH</td>
</tr>
<tr>
<td>Cisco ACI</td>
<td>SSH</td>
</tr>
<tr>
<td>Cisco Firepower</td>
<td>SSH</td>
</tr>
<tr>
<td>Cisco IOS</td>
<td>SSH</td>
</tr>
<tr>
<td>Citrix XenServer</td>
<td>SSH</td>
</tr>
<tr>
<td>Database</td>
<td>Database</td>
</tr>
<tr>
<td>Dell Force10 FTOS</td>
<td>SSH</td>
</tr>
<tr>
<td>Extreme ExtremeXOS</td>
<td>SSH</td>
</tr>
<tr>
<td>F5</td>
<td>F5</td>
</tr>
<tr>
<td>FireEye</td>
<td>SSH</td>
</tr>
<tr>
<td>Fortigate FortiOS</td>
<td>SSH</td>
</tr>
<tr>
<td>Generic SSH</td>
<td>SSH</td>
</tr>
<tr>
<td>HP ProCurve</td>
<td>SSH</td>
</tr>
<tr>
<td>Huawei VRP</td>
<td>SSH</td>
</tr>
<tr>
<td>IBM iSeries</td>
<td>IBM iSeries</td>
</tr>
<tr>
<td>Juniper Junos</td>
<td>SSH</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>Microsoft Azure</td>
</tr>
<tr>
<td>Mobile Device Manager</td>
<td>AirWatch, Apple Profile Manager, or Mobileiron</td>
</tr>
<tr>
<td>MongoDB</td>
<td>MongoDB</td>
</tr>
<tr>
<td>NetApp API</td>
<td>NetApp API</td>
</tr>
<tr>
<td>Office 365</td>
<td>Office 365</td>
</tr>
<tr>
<td>OpenStack</td>
<td>OpenStack</td>
</tr>
<tr>
<td>Product</td>
<td>Technology</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>NetApp Data ONTAP</td>
<td>SSH</td>
</tr>
<tr>
<td>Palo Alto Networks PAN-OS</td>
<td>PAN-OS</td>
</tr>
<tr>
<td>Rackspace</td>
<td>Rackspace</td>
</tr>
<tr>
<td>RHEV</td>
<td>RHEV</td>
</tr>
<tr>
<td>Salesforce.com</td>
<td>Salesforce SOAP API</td>
</tr>
<tr>
<td>SonicWALL SonicOS</td>
<td>SSH</td>
</tr>
<tr>
<td>Unix</td>
<td>SSH</td>
</tr>
<tr>
<td>Unix File Contents</td>
<td>SSH</td>
</tr>
<tr>
<td>VMware vCenter/vSphere</td>
<td>VMware ESX SOAP API or VMware vCenter SOAP API</td>
</tr>
<tr>
<td>WatchGuard</td>
<td>SSH</td>
</tr>
<tr>
<td>Windows</td>
<td>Windows</td>
</tr>
<tr>
<td>Windows File Contents</td>
<td>Windows</td>
</tr>
<tr>
<td>ZTE ROSNG</td>
<td>SSH</td>
</tr>
</tbody>
</table>
SCAP Settings in Vulnerability Management Scans

Note: If a scan is based on a user-defined template, you cannot configure SCAP settings in the scan. You can only modify these settings in the related user-defined template.

Security Content Automation Protocol (SCAP) is an open standard that enables automated management of vulnerabilities and policy compliance for an organization. It relies on multiple open standards and policies, including OVAL, CVE, CVSS, CPE, and FDCC policies.

If you create a scan or user-defined template based on the Tenable-provided SCAP and OVAL Auditing template, you must configure the SCAP settings.

Caution: SCAP scans in Tenable.io are unverified.

You can select Linux (SCAP), Linux (OVAL), Windows (SCAP), or Windows (OVAL). The settings for each option are described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux (SCAP) or Windows (SCAP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCAP File</td>
<td>None</td>
<td>A valid zip file that contains full SCAP content (XCCDF, OVAL, and CPE for versions 1.0 and 1.1; DataStream for version 1.2).</td>
</tr>
<tr>
<td>SCAP Version</td>
<td>1.2</td>
<td>The SCAP version that is appropriate for the content in the uploaded SCAP file.</td>
</tr>
<tr>
<td>SCAP Data Stream ID</td>
<td>None</td>
<td>(SCAP Version 1.2 only) The Data Stream ID that you copied from the SCAP XML file. Example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;data-stream id=&quot;scap_gov.nist_datastream_USGCB-Windows-7-1.2.3.1.zip&quot;&gt;</code></td>
</tr>
<tr>
<td>SCAP Benchmark ID</td>
<td>None</td>
<td>The Benchmark ID that you copied from the SCAP XML file.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>SCAP Profile ID</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Profile ID that you copied from the SCAP XML file.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;xccdf:Profile id=&quot;xccdf_gov.nist_profile_united_states_government_</td>
<td></td>
</tr>
<tr>
<td></td>
<td>configuration_baseline_version_</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.2.3.1&quot;</td>
<td></td>
</tr>
<tr>
<td>OVAL Result Type</td>
<td>Full results w/ system characteristics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The information you want the results file to include.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The results file can be one of the following types: full results with</td>
<td></td>
</tr>
<tr>
<td></td>
<td>system characteristics, full results without system characteristics, or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>thin results.</td>
<td></td>
</tr>
<tr>
<td><strong>Linux (OVAL) or Windows (OVAL)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OVAL definitions file</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A valid zip file that contains OVAL standalone content.</td>
<td></td>
</tr>
</tbody>
</table>
Configure Plugins in Vulnerability Management Scans

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can Configure

**Required Template Permissions:** Can Configure

**Note:** If a scan is based on a user-defined template, you cannot configure **Plugin** settings in the scan. You can only modify these settings in the related user-defined template.

**Note:** When Tenable adds new plugins to Tenable.io, the new plugins are automatically enabled if the entire plugin family they belong to is enabled in your scan policy template. If you only enabled some plugins from a family, you must manually enable new plugins to include them in your scan policy.

If you create a scan or user-defined template using the Tenable-provided **Advanced Scan** template, you can configure which security checks the scan performs by enabling or disabling plugins individually or by plugin family.

When you create and save a scan or user-defined template, it records all of the plugins that are initially selected. When new plugins are received via a plugin update, the plugins are automatically enabled if the family with which the plugins are associated is enabled. If the family has been disabled or partially enabled, new plugins in that family are also automatically disabled.

**Caution:** The **Denial of Service** family contains some plugins that could cause outages on a network if the **Safe Checks** option is not enabled, in addition to some useful checks that do not cause any harm. The **Denial of Service** family can be used in conjunction with **Safe Checks** to ensure that any potentially dangerous plugins are not run. However, it is recommended that the **Denial of Service** family not be used on a production network unless scheduled during a maintenance window and with staff ready to respond to any issues.

To configure plugins for a scan or user-defined template:

1. Do one of the following:
   
   a. [Create](#) or [edit](#) a scan.
   
   b. [Create](#) or [edit](#) a user-defined template.
2. In the left navigation list, click **Plugins**.

   The **Plugins** page appears. This page contains a table of plugin families.

3. Do one of the following:

   - **Filter** the plugin families table by various attributes.
   
   - **Search** the plugin families table by plugin family name. For more information on searching, see **Tenable.io Tables**.

4. To enable or disable all the plugins in a plugin family, click the **Status** toggle in row for the plugin family.

   - **On** – The scan includes the security checks associated with the plugin family.
   
   - **Off** – The scan excludes the security checks associated with the plugin family.

5. To enable or disable specific plugins for an individual plugin family:

   a. In the plugin families table, click the plugin family where you want to edit plugins. The plugin family plane appears.

   b. (Optional) Click an individual plugin to review plugin details (**Synopsis**, **Description**, and **Solution**).

   c. For each plugin you want to enable or disable, select or clear the **Status** checkbox.

   d. Click **Save**.

   The **Plugins** page appears. In the plugin families table, Tenable.io updates the plugin family status as follows:

   - **On** – If you enabled all plugins for the plugin family, the scan includes the security checks associated with the plugin family.
   
   - **Off** – If you disabled all plugins for the plugin family, the scan excludes the security checks associated with the plugin family.

   - **Mixed** – If you enabled only some of the plugins for the plugin family, the scan includes only the enabled plugins.

   e. Click **Save** to save your changes to the plugin family.
6. Click **Save** to save your changes to the scan or user-defined template.
Plugins (Classic Interface)

The Advanced Scan templates include Plugin options.

Plugins options enables you to select security checks by Plugin Family or individual plugins checks.

To enable/disable a plugin family:

1. Click Plugin Family to enable (green) or disable (gray) the entire family.

2. Select a family to display the list of its plugins.
   
   Individual plugins can be enabled or disabled to create very specific scans.

   **Note:** A family with some disabled plugins turns blue and displays Mixed to indicate only some plugins are enabled. Click on the plugin family to load the complete list of plugins, and allow for granular selection based on your scanning preferences.

3. Select a specific Plugin Name to display the plugin output that displays as seen in a report.
   
   The plugin details include a Synopsis, Description, Solution, Plugin Information, and Risk Information.

When you create and save a scan, it records all of the plugins that are initially selected. When new plugins are received via a plugin update, the plugins are automatically enabled if the family with which the plugins are associated is enabled. If the family has been disabled or partially enabled, new plugins in that family are also automatically disabled.

**Caution:** The Denial of Service family contains some plugins that could cause outages on a network if the Safe Checks option is not enabled, in addition to some useful checks that do not cause any harm. The Denial of Service family can be used in conjunction with Safe Checks to ensure that any potentially dangerous plugins are not run. However, it is recommended that the Denial of Service family not be used on a production network unless scheduled during a maintenance window and with staff ready to respond to any issues.
Plugin Settings in WAS Scans

**Required Tenable.io Web Application Scanning User Role:** Scan Manager or Administrator

Configure Plugin settings to specify the plugins and plugin families you want the scanner to use as it scans your web application.

When you create and launch a scan, Tenable.io Web Application Scanning uses plugins in various plugin families, each designed to identify certain types of findings or vulnerabilities, to analyze your web application. Tenable.io Web Application Scanning uses the 98000-98999 and 112290-117290 plugin ID ranges for scanning. For more information about Tenable.io Web Application Scanning plugin families, see the Web Application Scanning Plugin Families site.

**Note:** Tenable.io Web Application Scanning displays only the first detected 25 instances of an individual plugin per scan in your scan results. If you see 25 instances of a single plugin in your scan results, Tenable recommends taking remediation steps to address the corresponding vulnerability and then rescanning your target.

You can configure Plugin settings when you create a scan or user-defined scan template and select the **Overview** or **Scan** template type. However, the **Scan** template type has more plugin families to view and configure. For more information, see Scan Templates.

**Tip:** If you want to save your settings configurations and apply them to other scans, you can create and configure a user-defined scan template.

The plugins settings contains the following sections:

- All enabled
- Plugins table

**All Enabled**

A toggle you can click to enable or disable all plugins simultaneously.

**Plugins Table**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the plugin family to which the grouped</td>
<td>• View the name of each</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
<td>Actions</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>plugins belong.</td>
<td>plugin family.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Select the column to sort the alphabetically table by family name.</td>
</tr>
<tr>
<td>Total</td>
<td>Specifies the number of plugins in the plugin family.</td>
<td>• View the number of plugins in the family.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Select the column to sort the table by number of plugins in each family.</td>
</tr>
<tr>
<td>Status</td>
<td>Toggle that allows you to specify if you want the scanner to use the plugins in the plugin family to analyze your target.</td>
<td>• Click the <strong>Status</strong> toggle to disable the plugins in the plugin family.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) To enable a disabled plugin family, click the <strong>Status</strong> toggle.</td>
</tr>
</tbody>
</table>

In the plugins table, you can view details about or disable individual plugins.

**To view details about individual plugins:**

1. In the table, click the row for the family that contains a plugin you want to view.

   A plugin family details plane appears, displaying the name, ID, and status for each plugin in the family in a paginated list.

2. (Optional) To locate a specific plugin, in the **Search** box, type the name or ID.

3. Click the plugin for which you want to view details.

**To disable individual plugins:**
1. In the table, click the row for the family that contains the plugin you want to disable.

   A plugin family details plane appears, displaying the name, ID, and status for each plugin in the family in a paginated list.

2. (Optional) To locate a specific plugin, in the **Search** box, type the name or ID.

3. In the **Status** column, select the check box next to the plugin you want to disable.

4. (Optional) To enable a disabled plugin, select the check box.

5. Click **Save**.

   The details plane disappears.

   Tenable.io updates your plugin selections.
Target Groups

**Note:** This section describes the new interface. For information about the classic interface, see Target Groups (Classic Interface). For information about navigating the new interface, see Navigate Tenable.io (New Interface).

A target group allows you to construct a list of scan targets by FQDN, CIDR notation, or IP address range. You can then specify which users in your organization can use the target group in scan configurations or filtering dashboards (including workbenches).

**Note:** Tenable recommends limiting the number of targets in any single target group. When filtering a dashboard by a target group with too many targets, Tenable.io may fail to show data.

**Note:** System target groups and related functionality asset isolation are deprecated. To control scan permissions, use access groups instead.

You can still create and edit system target groups, as well as use system target groups in scan configurations and dashboard filters. However, Tenable recommends using user target groups instead.

If you grant a user permissions in a target group, the user can use the target group in the Target Groups option for scan configuration. However, you must also grant the user Can Scan permissions in an access group for the targets, or Tenable.io excludes the targets from the scan results. For more information, see Access Groups.

For more information on target groups, see the following topics:

- [Create a Target Group](#)
- [Configure User Permissions for a Target Group](#)
- [Edit a Target Group](#)
- [Import a Target Group](#)
- [Export a Target Group](#)
- [Delete a Target Group](#)
Create a Target Group

System target groups:

**Required User Role:** Administrator

User target groups:

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Note:** System target groups and related functionality asset isolation are deprecated. To control scan permissions, use **access groups** instead.

You can still create and edit system target groups, as well as use system target groups in scan configurations and dashboard filters. However, Tenable recommends using user target groups instead.

To create a target group in the new interface:

1. In the upper-left corner, click the **button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Target Groups** tile.

   The **Target Groups** page appears. By default, the **System** tab is active. This tab contains a table of system target groups.

4. If you want to edit a user target group, click **User**. Otherwise, stay on the **System** target groups tab.

5. In the upper-right corner of the page, click the **Create Target Group** button.

   The **Create a Target Group** page appears.

6. Configure the **General** settings:
### Setting | Description
--- | ---
**Name** | A name for the target group.
**Targets** | A comma-separated list of FQDNs, CIDR notation, or IP address ranges that you want to scan.
**Upload Targets** | A text file containing a comma-separated list of FQDNs or IP address ranges that you want to scan.

The system adds the uploaded targets to the **Targets** box after you save the target group.

7. **Configure** the user permissions for the group.

**Note:** If you grant a user permissions in a target group, the user can use the target group in the **Target Groups** option for scan configurations. However, you must also grant the user Can Scan permissions in an access group for the targets, or Tenable.io excludes the targets from the scan results. For more information, see **Access Groups**.

8. Click **Save**.

One of the following occurs:

- If you configured user permissions for the target group, Tenable.io creates the target group and adds it to the table on the **Target Groups** page.

- If you retained the default **No Access** permissions for the target group, a confirmation window appears.

In response, do one of the following:

- If the default configuration is appropriate for the target group, click **Continue** to confirm your action.

- If the default configuration is not appropriate for the target group, click **Cancel** to return to user permissions configuration for the target group.
Configure User Permissions for a Target Group

System target groups:

Required User Role: Administrator
Required Target Group Permissions: Any

User target groups:

Required Tenable.io Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator
Required Target Group Permissions: Can Change

Note: For auditing cloud infrastructure, Tenable.io requires a target group with Can Scan permissions to be present on 127.0.0.1.

Note: To enable the user to use a target group in the Target Groups option for scan configurations, you must also grant the user Can Scan permissions in an access group for the targets. If you do not, Tenable.io excludes the targets from the scan results. For more information, see Access Groups.

To configure permissions for a target group:

1. Create or edit a target group.
2. In the User Permissions section, do one of the following:
   - Change the permissions for the Default user.
     - Note: The Default user represents any users that have not been specifically added to the target group.
     a. Next to the permission drop-down for the Default user, click the ▼ button.
     b. Select a permissions level.
     c. Click Save.
   - Add permissions.
a. Next to **User Permissions**, click the **+** button.

   The **Add User Permission** plane appears.

b. In the **Add users or groups** box, type the name of a user or group.

   As you type, a filtered list of users and groups appears.

c. Select a user or group from the search results.

   The selected user or group appears in the list of users and groups.

   By default, Tenable.io assigns **Can Use** permissions to the new user or group.

d. Next to the permission drop-down for the user or group, click the **▼** button.

e. Select a **permissions level**.

f. Click **Save**.

• **Edit permissions.**

   a. Next to the permission drop-down for the user or group, click the **▼** button.

   b. Select a **permissions level**.

   c. Click **Save**.

• **Delete permissions.**

   a. In the list of users, roll over the user or group you want to delete.

   b. Click the **×** button next to the user or user group.

   The user or group disappears from the permissions list.

   c. Click **Save**.
Edit a Target Group

System target groups:

**Required User Role:** Administrator

**Required Target Group Permissions:** Any

User target groups:

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Target Group Permissions:** Can Change

**Note:** System target groups and related functionality asset isolation are deprecated. To control scan permissions, use access groups instead.

You can still create and edit system target groups, as well as use system target groups in scan configurations and dashboard filters. However, Tenable recommends using user target groups instead.

To edit a target group in the new interface:

1. In the upper-left corner, click the **button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The Settings page appears.

3. Click the **Target Groups** tile.
   
   The Target Groups page appears. By default, the **System** tab is active. This tab contains a table of system target groups.

4. If you want to edit a user target group, click **User**. Otherwise, stay on the **System** target groups tab.
5. In the target groups table, click the target group you want to edit.

   The **Update a Target Group** page appears.

6. Edit the **General** settings for the target group:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the target group.</td>
</tr>
<tr>
<td>Targets</td>
<td>A comma-separated list of FQDNs, CIDR notation, or IP address ranges that you want to scan.</td>
</tr>
<tr>
<td>Upload Targets</td>
<td>A text file containing a comma-separated list of FQDNs or IP address ranges that you want to scan. The system adds the uploaded targets to the <strong>Targets</strong> box after you save the target group.</td>
</tr>
</tbody>
</table>

7. **Configure** user permissions for the target group.

8. Click **Save**.

   A confirmation window appears.

9. In the confirmation window, click **Continue**.

   Tenable.io saves the changes to the target group.
Import a Target Group

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

You can import a target group as a `.csv` file.

**Tip:** To create or modify the `.csv` file, Tenable recommends using a robust editor such as Microsoft Excel.

Before you begin:

- Create a `.csv` file in the specified format.

To import a target group:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Target Groups** tile.

   The **Target Groups** page appears. By default, the **System** tab is active. This tab contains a table of system target groups.

4. If you want to import a user target group, click **User**. Otherwise, stay on the **System** target groups page.

**Note:** System target groups and related functionality asset isolation are deprecated. To control scan permissions, use **access groups** instead.

You can still create and edit system target groups, as well as use system target groups in scan configurations and dashboard filters. However, Tenable recommends using user target groups instead.

5. In the upper-right corner of the page, click the **Import** button.

   Your operating system's file manager appears.
6. Select a .csv file to import.

Tenable.io imports the file and adds the target groups to the target groups box.

Target Group Import File Format

Each line of the target group import file must have the following fields:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Numeric field used to identify the target group.</td>
</tr>
<tr>
<td>name</td>
<td>Field used to identify the name of the target group. Any combination of</td>
</tr>
<tr>
<td></td>
<td>alpha-numeric characters or symbols can be used in the name field.</td>
</tr>
<tr>
<td>members</td>
<td>Field used to identify host address(es) to be included in the target group.</td>
</tr>
<tr>
<td>creation_date</td>
<td>Numeric field in UNIX timestamp format.</td>
</tr>
<tr>
<td>last_modification_date</td>
<td>Numeric field in UNIX timestamp format.</td>
</tr>
</tbody>
</table>
Export a Target Group

Required Tenable.io Vulnerability Management User Role: Standard, Scan Manager, or Administrator

Required Target Group Permissions: Can Use

You can export a target group as a .csv file. Depending on your browser, the target group may download automatically.

To export a target group or groups in the new interface:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, click Settings.

   The Settings page appears.

3. Click the Target Groups tile.

   The Target Groups page appears. By default, the System tab is active. This tab contains a table of system target groups.

4. If you want to export a user target group, click User. Otherwise, stay on the System target groups tab.

   Note: System target groups and related functionality asset isolation are deprecated. To control scan permissions, use access groups instead.

   You can still create and edit system target groups, as well as use system target groups in scan configurations and dashboard filters. However, Tenable recommends using user target groups instead.

5. Select the target group or groups you want to export.

   • Select a single target group.

     a. In the target groups table, roll over the target group you want to export.

        The action buttons appear in the row.
b. In the row, click the button.

Tenable.io automatically exports the target group or groups you selected as a single .csv file.

- Select multiple target groups.
  a. In the target groups table, select the check boxes for each target group you want to export.
  The action bar appears at the bottom of the page.

b. Next to Target Groups, click the button.

Target Group Export File Header Fields

The following table describes the headers that appear in the exclusion export file.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Numeric identifier for the target group.</td>
</tr>
<tr>
<td>name</td>
<td>Alphanumeric name of the target group.</td>
</tr>
<tr>
<td>members</td>
<td>Host address(es) to be included in the target group.</td>
</tr>
<tr>
<td>creation_date</td>
<td>Date (in UNIX timestamp format) when the target group was created.</td>
</tr>
<tr>
<td>last_modification_date</td>
<td>Date (in UNIX timestamp format) when the target group was last modified.</td>
</tr>
</tbody>
</table>
Delete a Target Group

System target groups:

Required User Role: Administrator

Required Target Group Permissions: Any

User target groups:

Required Tenable.io Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

Required Target Group Permissions: Can Change

To delete a target group in the new interface:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, click Settings.

   The Settings page appears.

3. Click the Target Groups tile.

   The Target Groups page appears. By default, the System tab is active. This tab contains a table of system target groups.

4. If you want to delete a user target group, click User. Otherwise, stay on the System target groups tab.

5. Select the target group or groups you want to delete:

   - Select a single target group.
     
     a. In the target groups table, roll over the target group you want to delete.

     The action buttons appear in the row.
b. In the row, click the button.

A confirmation window appears.

- Select multiple target groups.
  a. In the target groups table, select the check box for each target group you want to delete.

  The action bar appears at the bottom of the page.

  b. In the action bar, click the button.

  A confirmation window appears.

6. In the confirmation window, click Delete.

  Tenable.io deletes the target group or groups you selected.
# Target Group Permissions

The following table describes user permissions for both system and user target groups.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Target Group</strong></td>
<td></td>
</tr>
<tr>
<td>No Access</td>
<td>(Default user only) Users assigned this permission cannot use the system target group to filter dashboards.</td>
</tr>
</tbody>
</table>
| Can Use    | Users assigned this permission can use hosts in the user target groups to filter dashboards and configure scans.  

**Note:** System target groups are deprecated; Tenable recommends using user target groups instead.

**Note:** To enable the user to use a target group in the **Target Groups** option for scan configurations, you must also grant the user **Can Scan** permissions in an access group for the targets. If you do not, Tenable.io excludes the targets from the scan results. For more information, see **Access Groups**.

<table>
<thead>
<tr>
<th><strong>User Target Group</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No Access</td>
<td>(Default user only) Users assigned this permission cannot configure scans for hosts in the user target group or use hosts in the user target group to filter dashboards.</td>
</tr>
</tbody>
</table>
| Can Use               | Users assigned this permission can use hosts in the user target groups to filter dashboards and configure scans.  

**Note:** To enable the user to use a target group in the **Target Groups** option for scan configurations, you must also grant the user **Can Scan** permissions in an access group for the targets. If you do not, Tenable.io excludes the targets from the scan results. For more information, see **Access Groups**.

| Can Change            | In addition to using hosts in this user target group when configuring scans and filtering dashboards, users assigned this permission can modify any setting for the target group except permissions. |
Target Groups (Classic Interface)

**Note:** System target groups and related functionality asset isolation are deprecated. To control scan permissions, use **access groups** instead.

You can still create and edit system target groups, as well as use system target groups in scan configurations and dashboard filters. However, Tenable recommends using user target groups instead.

A target group allows you to construct a list of scan targets by FQDN, CIDR notation, or IP address range. You can then specify which users in your organization can use the target group in **scan configurations** or **filtering** dashboards (including workbenches).

If you grant a user permissions in a target group, the user can use the target group in the **Target Groups** option for scan configuration. However, you must also grant the user **Can Scan** permissions in an access group for the targets, or Tenable.io excludes the targets from the **scan results**. For more information, see **Access Groups**.

For more information on target groups, see the following topics:

- [Create a Target Group](#)
- [Configure User Permissions for a Target Group](#)
- [Edit a Target Group](#)
- [Import a Target Group](#)
- [Export a Target Group](#)
- [Delete a Target Group](#)
Create a Target Group (Classic Interface)

System target groups:

**Required User Role:** Administrator

User target groups:

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

To create a target group:

1. In the top navigation bar, click **Scans**.
   
The **My Scans** page appears.

2. In the left navigation bar, click **Target Groups**.
   
The **Target Groups** page appears. By default, the **System** tab is active. This tab contains a table of system target groups.

   **Note:** System target groups and related functionality asset isolation are deprecated. To control scan permissions, use **access groups** instead.

   You can still create and edit system target groups, as well as use system target groups in scan configurations and dashboard filters. However, Tenable recommends using user target groups instead.

3. Click the **User** tab.
   
   A table of user target groups appears.

4. In the upper-right corner of the page, click the **New Group** button.
   
The **New Target Group** page appears. By default, the **Settings** tab is active.

5. In the **Name** box, type a name for the target group.

6. In the **Targets** box, type a comma-separated list of asset identifiers that you want to filter dashboards on.
Supported identifiers include FQDNs, CIDR notation, or IP address ranges.

7. (Optional) Upload a file of asset identifiers you want to filter dashboards on.
   a. Next to Upload, click Add File.
   b. Navigate to and select the text file of a comma-separated list of FQDNs or IP address ranges that you want to filter dashboards on.

   Tenable.io adds the uploaded identifiers to the Targets box after you save the target group.

8. Configure user permissions for the target group.

   **Note:** If you grant a user permissions in a target group, the user can use the target group in the Target Groups option for scan configurations. However, you must also grant the user Can Scan permissions in an access group for the targets, or Tenable.io excludes the targets from the scan results. For more information, see Access Groups.

9. Click Save.

   One of the following occurs:
   
   - If you configured user permissions for the target group, Tenable.io creates the target group and adds it to the table on the Target Groups page.
   - If you retained No Access permissions for the Default user, a confirmation window appears.

   In response, do one of the following:

   - If the default configuration is appropriate for the target group, click Continue to confirm your action.
   - If the default configuration is not appropriate for the target group, click Cancel to return to user permissions configuration for the target group.
Configure Permissions for a Target Group (Classic Interface)

System target groups:

Required User Role: Administrator

Required Target Group Permissions: Any

User target groups:

Required Tenable.io Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

Required Target Group Permissions: Can Change

Note: To enable the user to use a target group in the Target Groups option for scan configurations, you must also grant the user Can Scan permissions in an access group for the targets. If you do not, Tenable.io excludes the targets from the scan results. For more information, see Access Groups.

To configure permissions for a user target group:

1. Create or edit a target group.

2. Click the Permissions tab.

3. In the Permissions section, do one of the following:

   Tip: Tenable recommends assigning permissions to user groups, rather than individual users, to minimize maintenance as individual users leave or join your organization.

   • Add permissions for a user or user group.
     a. In the Add users or groups box, type the name of a user or group.

     As you type, a filtered list of users and groups appears.

     Note: The Default user represents any users that have not been specifically added to the target group.
b. Select a user or group from the search results.

   Tenable.io adds the user to the permissions list, with a default permission of **Can Use**.

c. **(Optional) For user target groups:**
   i. Next to the permissions drop-down for the user or group, click the ▼ button.

   ii. Select a **permissions level**.

d. Click **Save**.

   Tenable.io adds permissions for the specified user or group.

- **Edit permissions for a user or user group.**
  a. Next to the permission drop-down for the user or group, click the ▼ button.

  b. Select a **permissions level**.

  c. Click **Save**.

   Tenable.io saves the modified permissions.

- **Delete permissions for a user or user group.**
  a. In the permissions list, next to the user or group you want to delete, click the ✗ button.

   The user or group disappears from the permissions list, but is not permanently removed from the target group yet.

  b. Click **Save**.

   Tenable.io removes the user or group from the target group.
Edit a Target Group (Classic Interface)

System target groups:

<table>
<thead>
<tr>
<th>Required User Role:</th>
<th>Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required Target Group Permissions:</td>
<td>Any</td>
</tr>
</tbody>
</table>

User target groups:

<table>
<thead>
<tr>
<th>Required Tenable.io Vulnerability Management User Role:</th>
<th>Scan Operator, Standard, Scan Manager, or Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required Target Group Permissions:</td>
<td>Can Change</td>
</tr>
</tbody>
</table>

To edit a target group:

1. In the top navigation bar, click **Scans**.
   
The **My Scans** page appears.

2. In the left navigation bar, click **Target Groups**.
   
The **Target Groups** page appears. By default, the **System** tab is active. This tab contains a table of system target groups.

   **Note:** System target groups and related functionality asset isolation are deprecated. To control scan permissions, use **access groups** instead.

   You can still create and edit system target groups, as well as use system target groups in scan configurations and dashboard filters. However, Tenable recommends using user target groups instead.

3. Click the **User** tab.

4. In the target group table, click the target group you want to modify.
   
The **Edit Target Group** page appears. By default, the **Settings** tab is active.

5. In the **Name** box, type a name for the target group.
6. In the **Targets** box, type a comma-separated list of asset identifiers that you want to filter dashboards on.

   Supported identifiers include FQDNs, CIDR notation, or IP address ranges.

7. (Optional) Upload a file of asset identifiers you want to filter dashboards on.
   
   a. Next to **Upload**, click **Add File**.
   
   b. Navigate to and select the text file of a comma-separated list of FQDNs or IP address ranges that you want to filter dashboards on.

   Tenable.io adds the uploaded identifiers to the **Targets** box after you save the target group.

8. [Configure](#) user permissions for the target group.

9. Click **Save**.

   A confirmation window appears.

10. Click **Continue** to confirm your action.

    Tenable.io saves the changes to the target group.
Import a Target Group (Classic Interface)

**Required User Role:** Administrator

You can import a target group as a .csv file.

**Tip:** To create or modify the .csv file, Tenable recommends using a robust .csv editor, such as Microsoft Excel.

Before you begin:

- Create a .csv file with the following fields in each line:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Numeric field used to identify the target group.</td>
</tr>
<tr>
<td>name</td>
<td>Field used to identify the name of the target group. Any combination of alpha-numeric characters or symbols can be used in the <strong>name</strong> field.</td>
</tr>
<tr>
<td>members</td>
<td>Field used to identify host address(es) to be included in the target group.</td>
</tr>
<tr>
<td>creation_date</td>
<td>Numeric field in UNIX timestamp format.</td>
</tr>
<tr>
<td>last_modification_date</td>
<td>Numeric field in UNIX timestamp format.</td>
</tr>
</tbody>
</table>

To import a target group:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Target Groups**.
   
   The **Target Groups** page appears. By default, the **System** tab is active. This tab contains a table of system target groups.
Note: System target groups and related functionality asset isolation are deprecated. To control scan permissions, use access groups instead.

You can still create and edit system target groups, as well as use system target groups in scan configurations and dashboard filters. However, Tenable recommends using user target groups instead.

3. Click the **User** tab.

   A table of user target groups appears.

4. In the upper-right corner of the page, click the **Import** button.

   The file explorer for your operating system appears.

5. Select a file to import.

   Tenable.io adds the new target group. The target group appears in the list of groups.
Export a Target Group (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Standard, Scan Manager, or Administrator

**Required Target Group Permissions:** Can Use

You can export a target group as a .csv file. Depending on your browser, the target group may download automatically.

**To export a single target group:**

1. In the top navigation bar, click **Scans**.

   The **My Scans** page appears.

2. In the left navigation bar, click **Target Groups**.

   The **Target Groups** page appears. By default, the **System** tab is active. This tab contains a table of system target groups.

   **Note:** System target groups and related functionality asset isolation are deprecated. To control scan permissions, use **access groups** instead.

   You can still create and edit system target groups, as well as use system target groups in scan configurations and dashboard filters. However, Tenable recommends using user target groups instead.

3. Click the **User** tab.

   A table of user target groups appears.

4. In the target group table, click the **arrow** button next to the target group you want to export.

   The target group downloads as a .csv file. Depending on your browser, this download may be automatic.

**To export multiple target groups:**

1. In the top navigation bar, click **Scans**.

   The **My Scans** page appears.
2. In the left navigation bar, click **Target Groups**.

   The **Target Groups** page appears. By default, the **System** tab is active. This tab contains a table of system target groups.

   **Note:** System target groups and related functionality asset isolation are deprecated. To control scan permissions, use **access groups** instead.

   You can still create and edit system target groups, as well as use system target groups in scan configurations and dashboard filters. However, Tenable recommends using user target groups instead.

3. Click the **User** tab.

   A table of user target groups appears.

4. In the target group table, select the check boxes next to the target groups you want to export.

5. In the upper-right corner, click the **Export** button.

   The target groups download in a single .csv file. Depending on your browser, this download may be automatic.

**Target Group Export File Format**

The following table displays the fields that appear in the target group export file.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Numeric field used to identify the target group.</td>
</tr>
<tr>
<td>name</td>
<td>Field used to identify the name of the target group. Any combination of</td>
</tr>
<tr>
<td></td>
<td>alpha-numeric characters or symbols can be used in the <strong>name</strong> field.</td>
</tr>
<tr>
<td>members</td>
<td>Field identifying host address(es) to be included in the target group.</td>
</tr>
<tr>
<td>creation_date</td>
<td>Date field in UNIX timestamp format.</td>
</tr>
<tr>
<td>last_modification_date</td>
<td>Date field in UNIX timestamp format.</td>
</tr>
</tbody>
</table>
Delete a Target Group (Classic Interface)

System target groups:

- **Required User Role:** Administrator
- **Required Target Group Permissions:** Any

User target groups:

- **Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator
- **Required Target Group Permissions:** Can Change

To delete a single target group:

1. In the top navigation bar, click **Scans**. The **My Scans** page appears.
2. In the left navigation bar, click **Target Groups**. The **Target Groups** page appears. By default, the **System** tab is active. This tab contains a table of system target groups.
3. If you want to delete a user target group, click **User**. Otherwise, stay on the **System** target groups tab.
4. In the target group table, click the **Delete** button next to the target group you want to delete. A confirmation window appears.
5. Click the **Delete** button to confirm your action. Tenable.io deletes the target group.

To delete multiple target groups:

1. In the top navigation bar, click **Scans**. The **My Scans** page appears.
2. In the left navigation bar, click **Target Groups**.

   The **Target Groups** page appears. By default, the **System** tab is active. This tab contains a table of system target groups.

3. Depending on the type of target groups you want to delete, click the **System** or **User** tab.

4. In the target groups table, select the check boxes next to the target groups you want to delete.

5. In the upper-right corner, click the **Delete** button.

   A confirmation window appears.

6. Click the **Delete** button to confirm your action.

   Tenable.io deletes the target groups you selected.
Exclusions

**Note:** This section describes the new interface. For information about the classic interface, see [Exclusions (Classic Interface)](#). For information about navigating the new interface, see [Navigate Tenable.io (New Interface)](#).

You can use exclusions to restrict the scanning of specific hosts based on a selected schedule.

For more information on exclusions, see the following topics:

- [Create an Exclusion](#)
- [Edit an Exclusion](#)
- [Import an Exclusion](#)
- [Export an Exclusion](#)
- [Delete an Exclusion](#)
- [Exclusion Settings](#)
- [Exclusions (Classic Interface)](#)
Create an Exclusion

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

To create an exclusion in the new interface:

1. In the upper-left corner, click the ☰ button.
   
The left navigation plane appears.
2. In the left navigation plane, click **Settings**.
   
The **Settings** page appears.
3. Click the **Exclusions** tile.
   
The **Exclusions** page appears.
4. In the upper-right corner of the page, click the ☀️ **Create Exclusion** button.
   
The **Create an Exclusion** page appears.
5. Set the **exclusion settings**.
6. Click **Save**.

Tenable.io saves the exclusion and applies the exclusion to the selected scan targets.
Edit an Exclusion

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

To edit an exclusion in the new interface:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Exclusions** tile.
   
   The **Exclusions** page appears.

4. In the exclusions table, click the exclusion you want to edit.
   
   The **Update an Exclusion** page appears.

5. Edit the **exclusion settings**.

6. Click **Save**.

   Tenable.io saves the exclusion, and the **Exclusions** page appears.
Import an Exclusion

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

You can import an exclusion as a .csv file.

**Note:** When you import an exclusion, Tenable.io automatically assigns it to the default network. After import, you can move the exclusion to a custom network.

**Tip:** To create or modify the .csv file, Tenable.io recommends using a robust editor such as Microsoft Excel.

Before you begin:

- Create a .csv file in the specified format.

To import an exclusion:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Exclusions** tile.

   The **Exclusions** page appears.

4. In the upper-right corner of the page, click the button.

   Your operating system's file manager appears.

5. Select a .csv file to import.

   Tenable.io imports the file and adds the exclusions to the exclusions table.
Exclusion Import File

You can import one or more exclusions as a .csv file.

**Note:** Tenable does not recommend opening the .csv file in Microsoft Excel, as Excel adds additional characters to the file that Tenable.io cannot recognize.

This file is composed of a header and at least one line of data. Each line in the file must be separated by a new line break.

**Header (Optional)**

A header line in the file is optional. If included, the header must be the first line in the file and be formatted as follows:

```
id,name,description,members,creation_date,last_modification_date
```

**Note:** There are no spaces after the commas.

**Data (Required)**

Each data line in the file represents one exclusion configuration. Data lines must be separated from each other by a new line break. The file must include at least one data line.

Each data line is a comma-delimited string of fields described in the table below.

**Note:** Optional fields can be blank, but the associated comma separator must be present in the data line.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>An integer that uniquely identifies the exclusion.</td>
<td>No</td>
</tr>
<tr>
<td>name</td>
<td>The name of the exclusion. You can use any combination of alpha-numeric characters or symbols.</td>
<td>Yes</td>
</tr>
<tr>
<td>description</td>
<td>A description for the exclusion.</td>
<td>Yes</td>
</tr>
<tr>
<td>members</td>
<td>The target or targets where you want the scan exclusion to apply.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
This value can have the following formats:

- A host name (example.com)
- An IP address (192.0.2.57)
- An IP range (192.0.2.57-192.0.2.67)
- A comma-separated list of multiple host names, IP addresses, or IP ranges, bracketed by quotation marks ("192.0.2.57,192.0.2.177,192.0.2.8")

<table>
<thead>
<tr>
<th>creation_date</th>
<th>The Unix timestamp that Tenable.io uses as the creation date for the imported exclusion.</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>last_modification_date</td>
<td>The Unix timestamp that Tenable.io uses as the last modification date for the exclusion.</td>
<td>No</td>
</tr>
</tbody>
</table>

**Example**

```plaintext
id,name,description,members,creation_date,last_modification_date
1,Exclusion Rule 1,router-s,"192.0.2.57,192.0.21.177,192.0.28",1561643735,1561643785,Exclusion Rule 2,workstations,192.0.257-192.0.267,
```
Export an Exclusion

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

You can export an exclusion as a .csv file. Depending on your browser, the exclusion may download automatically.

To export a single exclusion in the new interface:

1. In the upper-left corner, click the ** button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Exclusions** tile.
   
   The **Exclusions** page appears.

4. Select the exclusions you want to export:
   
   - **Select a single exclusion:**
     
     a. In the exclusions table, roll over the exclusion you want to export.
        
        The action buttons appear in the row.
     
     b. In the row, click the [→] button.
   
   - **Select multiple exclusions:**
     
     a. In the exclusions table, select the check boxes next to each exclusion you want to export.
        
        The action bar appears at the bottom of the page.
     
     b. In the action bar, click the [→] button.
        
        The exclusions download automatically in one .csv file.

   Tenable.io automatically exports the selected exclusion or exclusions as a .csv file.
Exclusion Export File Header Fields

The following table describes the headers that appear in the exclusion export file.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Numeric identifier for the exclusion.</td>
</tr>
<tr>
<td>name</td>
<td>Alphanumeric name of the exclusion.</td>
</tr>
<tr>
<td>members</td>
<td>Host address(es) to be included in the exclusion.</td>
</tr>
<tr>
<td>creation_date</td>
<td>Date (in UNIX timestamp format) when the exclusion was created.</td>
</tr>
<tr>
<td>last_modification_date</td>
<td>Date (in UNIX timestamp format) when the exclusion was last modified.</td>
</tr>
</tbody>
</table>
Delete an Exclusion

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

To delete an exclusion or exclusions in the new interface:

1. In the upper-left corner, click the ⌔ button.
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   The **Settings** page appears.

3. Click the **Exclusions** tile.
   The **Exclusions** page appears.

4. Select the exclusion or exclusions you want to delete:
   - **Select a single exclusion.**
     a. In the exclusions table, roll over the exclusion you want to delete.
        The action buttons appear in the row.
     b. In the row, click the 🔴 button.
        A confirmation window appears.
   - **Select multiple exclusions.**
     a. In the exclusions table, select the check box for each exclusion you want to delete.
        The action bar appears at the bottom of the page.
     b. In the action bar, click the 🔴 button.
        A confirmation window appears.

5. In the confirmation window, click **Delete**.
   Tenable.io deletes the selected exclusion or exclusions.
## Exclusion Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Specifies a name for the exclusion.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies a description for the exclusion.</td>
</tr>
<tr>
<td>Targets</td>
<td>Specifies targets that you want excluded from scans. Enter targets as host names or IP ranges, separated by commas.</td>
</tr>
<tr>
<td>Network</td>
<td>Specifies the network that the targets belong to: either Default or a custom network.</td>
</tr>
<tr>
<td>Upload Targets</td>
<td>Uploads a text file with host names or IP ranges, separated by commas, that you want excluded from scans.</td>
</tr>
<tr>
<td><strong>Schedule</strong></td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>Enables or disables a schedule for when the exclusion is enabled. When disabled, the exclusion is set to Always On. When enabled, you can configure the following settings, which set a frequency and schedule for when the exclusion is enabled.</td>
</tr>
<tr>
<td>Summary</td>
<td>A summary of the selections for the Frequency, Starts, and Ends settings.</td>
</tr>
<tr>
<td>Frequency</td>
<td>A drop-down box that contains the following options: Once, Daily, Weekly, Monthly, and Yearly.</td>
</tr>
<tr>
<td>Starts</td>
<td>Two drop-down boxes in which you can select a date and time when the exclusion begins.</td>
</tr>
<tr>
<td>Ends</td>
<td>Two drop-down boxes in which you can select a date and time when the exclusion ends.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>A drop-down box with a search bar in which you can select a time zone for the selected dates and times.</td>
</tr>
</tbody>
</table>
Exclusions (Classic Interface)

You can use exclusions to restrict the scanning of specific hosts based on a selected schedule. Exclusions without a schedule are set to Always On.

**Note:** Exclusions in Tenable.io apply to Nessus scans only.

To access the Exclusions page, in the top navigation bar, click **Scans**, then in the left navigation bar, click **Exclusions**.

### Exclusion Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a name for the exclusion.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies a description for the exclusion.</td>
</tr>
<tr>
<td>Targets</td>
<td>Specifies targets that you want excluded from scans. Enter targets as host names or IP ranges, separated by commas.</td>
</tr>
<tr>
<td>Network</td>
<td>Specifies the network that the targets belong to: either <strong>Default</strong> or a custom network.</td>
</tr>
<tr>
<td>Upload Tar-</td>
<td>Uploads a text file with host names or IP ranges, separated by commas, that</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>gets</td>
<td>you want excluded from scans.</td>
</tr>
</tbody>
</table>

**Schedule**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>A toggle to enable or disable the exclusion. When set to <strong>On</strong>, the following options appear that allow you to select a time span for when the exclusion is enabled.</td>
</tr>
<tr>
<td>Frequency</td>
<td>A drop-down box that contains the following options: <strong>Once</strong>, <strong>Daily</strong>, <strong>Weekly</strong>, <strong>Monthly</strong>, and <strong>Yearly</strong>.</td>
</tr>
<tr>
<td>Starts</td>
<td>Two drop-down boxes in which you can select a date and time when the exclusion begins.</td>
</tr>
<tr>
<td>Ends</td>
<td>Two drop-down boxes in which you can select a date and time when the exclusion ends.</td>
</tr>
<tr>
<td>Timezone</td>
<td>A drop-down box with a search bar in which you can select a time zone for the selected dates and times.</td>
</tr>
</tbody>
</table>

**Summary**

A summary of the selections for the **Frequency**, **Starts**, **Ends**, and **Timezone** settings.

For more information on **Exclusions**, see the following topics:

- [Create an Exclusion (Classic Interface)]
- [Edit an Exclusion (Classic Interface)]
- [Import an Exclusion (Classic Interface)]
- [Export an Exclusion (Classic Interface)]
- [Delete an Exclusion (Classic Interface)]
Create an Exclusion (Classic Interface)

Required Tenable.io Vulnerability Management User Role: Scan Manager or Administrator

To create an exclusion:

1. In the top navigation bar, click **Scans**.
   The **My Scans** page appears.

2. In the left navigation bar, click **Exclusions**.
   The **Exclusions** page appears.

3. In the upper-right corner, click the **New Exclusion** button.
   The **New Exclusion** page appears, where you can manage **exclusion settings**.
Edit an Exclusion (Classic Interface)

Required Tenable.io Vulnerability Management User Role: Scan Manager or Administrator

To edit an exclusion:

1. In the top navigation bar, click **Scans**.
   The **My Scans** page appears.

2. In the left navigation bar, click **Exclusions**.
   The **Exclusions** page appears.

3. In the exclusions table, click the exclusion you want to edit.
   The **Edit Exclusion** page appears.

4. Edit the **exclusion settings**.
Import an Exclusion (Classic Interface)

Required Tenable.io Vulnerability Management User Role: Scan Manager or Administrator

You can import exclusion configurations as a comma-separated values (.csv) file. For more information on the file format, see Exclusion Import File.

Note: When you import an exclusion, Tenable.io automatically assigns it to the default network. After import, you can move the exclusion to a custom network.

Tip: To create or modify the CSV file, use a robust text editor such as TextMate (Mac), VIM (Linux), or NotePad++ (Windows).

To import an exclusion:

1. In the top navigation bar, click Scans.
   
   The My Scans page appears.

2. In the left navigation bar, click Exclusions.
   
   The Exclusions page appears.

3. In the upper-right corner, click the Import button.
   
   Your file explorer appears.

4. Select a .csv exclusion file to import.
   
   The exclusion appears in the list of exclusions.
Export an Exclusion (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

You can export an exclusion as a comma separate values (.csv) file. Depending on your browser, the exclusion may download automatically.

The following table displays the headers that will appear in the exclusion file.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Numeric field used to identify the exclusion.</td>
</tr>
<tr>
<td>name</td>
<td>Field used to identify the name of the exclusion. Any combination of alpha-</td>
</tr>
<tr>
<td></td>
<td>numeric characters or symbols can be used in the name field.</td>
</tr>
<tr>
<td>members</td>
<td>Field identifying host address(es) to be included in the exclusion.</td>
</tr>
<tr>
<td>creation_date</td>
<td>Date field in UNIX timestamp format.</td>
</tr>
<tr>
<td>last_modification_date</td>
<td>Date field in UNIX timestamp format.</td>
</tr>
</tbody>
</table>

To export one or more exclusions:

To export an exclusion:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Exclusions**.
   
   The **Exclusions** page appears.

3. In the list of exclusions, click the ↓ button next to the exclusion you want to export.

   The exclusion downloads automatically in .csv format.

To export multiple exclusions:
1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Exclusions**.
   
   The **Exclusions** page appears.

3. In the list of exclusions, select the check boxes next to the exclusions you want to export.

4. In the upper-right corner, click the **Export** button.
   
   The exclusions download automatically in one .csv file.
Delete an Exclusion (Classic Interface)

Required Tenable.io Vulnerability Management User Role: Scan Manager or Administrator

To delete an exclusion:

1. In the top navigation bar, click **Scans**.
   - The **My Scans** page appears.
2. In the left navigation bar, click **Exclusions**.
   - The **Exclusions** page appears.
3. In the list of exclusions, click the × button next to the exclusion you want to delete.
   - The **Delete Exclusion** window appears, prompting you to confirm the deletion.
4. Click the **Delete** button.
   - Tenable.io deletes the exclusion.

To delete multiple exclusions:

1. In the top navigation bar, click **Scans**.
   - The **My Scans** page appears.
2. In the left navigation bar, click **Exclusions**.
   - The **Exclusions** page appears.
3. In the list of exclusions, select the check boxes next to the exclusions you want to delete.
4. In the upper-right corner, click the **Delete** button.
   - The **Delete Exclusions** window appears, prompting you to confirm the deletion.
5. Click the **Delete** button.
   - Tenable.io deletes the exclusions.
Scans (Classic Interface)

On the Scans page, you can create, view, and manage scans and resources.

When you access the Scans page, the My Scans folder appears by default. A list of scans appears in the center pane. This documentation refers to the list as the scans table.

In each folder on the Scans page, the scans table displays the scans stored in that folder and the status of each scan. You can use the scans table to view the results of a scan, view the scan’s schedule, view the scan’s last modified date, and launch or delete a scan.

**Note:** Scans owned by disabled users cannot launch. Scans running at the time a user is disabled continue to run.

**Tip:** For more information on how to work with scans, refer to Scanning Overview (Classic Interface).

For more information, see the following sections:

- Scan Folders (Classic Interface)
- Tenable-Provided Scanner Templates (Classic Interface)
- WAS Scan Templates
- Scan Settings, Credentials, Compliance, SCAP, and Plugins.
- Create and Manage Scans (Classic Interface)
- Policies (Classic Interface)
- Target Groups (Classic Interface)
- Exclusions (Classic Interface)
- Scanners (Classic Interface)
- Agents (Classic Interface)

**Note:** For information about scanners and agents in the new interface, see Sensors and Agents.
Scanning Overview (Classic Interface)

Configure scans to collect data for Tenable.io. This overview walks you through the main steps you need to create, configure, launch, and manage scans.

Depending on your organization, one person may perform all of the steps, or several people may share the steps.

Create and launch an assessment scan

**Video:** [Launch a Basic Network Scan in Tenable.io](#)

1. [Create a scan](#).
2. Select a scan template that fits your needs.
   - Use a [Tenable-provided scanner template](#).
   - Use a [Tenable-provided agent template](#).
   - Create and use a [policy](#).
3. Configure the scan:
   - Configure the [scan settings](#) available for your template.
     For information about scan targets, see [Scan Targets](#).
   - (Optional) To run a credentialed scan, configure [credentials](#).
   - (Optional) To run a compliance scan, select the [compliance audits](#) your scan includes.
   - (Optional) If you are using an advanced scan template, select what [plugins](#) your scan includes.
4. [Launch the scan](#).

View and manage scans
1. **View your scans.**
   - View results for a specific scan.
   - Manage scan folders.

2. To analyze data across all your scan results, see **Analysis**.

**Refine scanning settings**

- Use **exclusions** to restrict the scanning of specific hosts based on a selected schedule.
- Use **target groups** to set permissions on which hosts a user can scan.
- To understand scan distribution concepts such as scanner capacity, job queues, and how Tenable.io dispatches tasks, see **Scan Distribution**.
## Scan Status (Classic Interface)

In Tenable.io, depending on its state, scans can have following status indicators:

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>The latest run of the scan is complete.</td>
</tr>
<tr>
<td>⚡</td>
<td>The latest run of the scan is incomplete, because Tenable.io or the scanner encountered problems during the run and aborted the scan. For more information about the problems encountered during the run, view the scan notes.</td>
</tr>
<tr>
<td>⏩</td>
<td>A user imported the scan. You cannot run imported scans. Scan history is unavailable for imported scans.</td>
</tr>
<tr>
<td>📅</td>
<td>The scan is either empty (the scan is new or has yet to run) or pending (Tenable.io is processing a request to run the scan).</td>
</tr>
<tr>
<td>⌁</td>
<td>The scan is currently running, or the scan is in the process of resuming after a user paused the run.</td>
</tr>
<tr>
<td>⏸️</td>
<td>At user request, Tenable.io successfully stopped the latest run of the scan. Tenable.io categorizes the scan as canceled.</td>
</tr>
<tr>
<td>⏳️</td>
<td>A user paused the scan. This indicator is present even if Tenable.io is still processing the action.</td>
</tr>
<tr>
<td>🔒</td>
<td>A user stopped the scan, and Tenable.io is processing the action.</td>
</tr>
</tbody>
</table>
Create and Manage Scans (Classic Interface)

To manage your scans, you can perform actions in the following areas.

Scan Configuration

- [Create a Scan (Classic Interface)]
- [Create an Agent Scan (Classic Interface)]
- [Edit a Scan Configuration (Classic Interface)]
- [Copy a Scan Configuration (Classic Interface)]
- [Change Scan Ownership (Classic Interface)]
- [Manage Scan Folders (Classic Interface)]
- [Move a Scan to the Trash Folder (Classic Interface)]
- [Delete a Scan (Classic Interface)]

Scan Operation

- [View Scans (Classic Interface)]
- [Launch a Scan (Classic Interface)]
- [Pause or Resume a Scan (Classic Interface)]
- [Start or Stop a Scan (Classic Interface)]

Scan Results

- [Import a Scan (Classic Interface)]
- [View Results for an Individual Scan (Classic Interface)]
- [View Scan Notes (Classic Interface)]
- [View Vulnerability Details for an Individual Scan (Classic Interface)]
- [Export Scan Results (Classic Interface)]
Create a Scan (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Note:** As a scan operator, you can only create a scan using user-defined policies that are shared with you.

When you create a scan, Tenable.io assigns you owner permissions for the scan.

Before you begin:

- Refer to the [scan templates documentation](#) for descriptions, available settings, and credentials for each Tenable.io scan template.

- Create an access group for any targets you want to use in the scan and assign Can Scan permissions to the appropriate users.

To create a scan:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the upper-right corner, click the **New Scan** button.
   
   The **Scan Templates** page appears.

3. Click the scan template that you want to use.

4. Configure the scan:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Settings</strong></td>
<td>Configure the <strong>settings</strong> for the template you chose. Settings include basic settings like scan name, targets, and scanner used, as well as more advanced settings you can use to refine the scan.</td>
</tr>
</tbody>
</table>
## Compliance/SCAP

Specify which **platforms** you want to audit. Tenable, Inc. provides best practice audits for each platform. Additionally, you can upload a custom audit file.

## Plugins

Select security checks by plugin family or individual **plugin**.

## Credentials

**Note:** Any credentials added to a scan (managed or scan-specific) override policy-specific credentials.

Specify options to perform a credentialed scan:

- To add a managed credential, under **Add Managed Credentials**, click **Add**.
  
  For more information, see [Add or Edit Managed Credentials for a Scan (Classic Interface)](https://tenable.io/docs/).  

- To add a scan-specific credential (that is, a credential used only by this scan):
  
  a. Under **Add Credentials**, click a credential type.  
  b. Configure the **credential settings**.

5. Do one of the following:

- If you want to launch the scan later, click **Save**.
  Tenable.io saves the scan.

- If you want to launch the scan immediately:
  
  a. Click the **button**.

  b. Click **Launch**.

    Tenable.io launches and saves the scan.
Create a Limited Plugin WAS Scan (Classic Interface)

**Required Additional License:** Tenable.io Web Application Scanning

To create a limited plugin scan in the classic interface:

1. In the top navigation bar, click **Scans**.
   The **My Scans** page appears.
2. In the upper right corner, click **New Scan**.
   The **Scan Templates** page appears.
3. Click the **Web Application** tab.
4. Click **Web App Overview** or **Web App Scan**.
5. Click the **Plugins** tab.
   The list of plugin families appears, and, by default, all of the plugin families are enabled.

   ![Plugin List](image)

6. In the upper right corner, click **Disable All**.

---

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective
All plugin families are disabled.

7. Click the plugin family that you want to include.

The list of plugins appears in the right pane.
8. For each plugin that you want to enable, click the **Disabled** button.

Each plugin is enabled.

<table>
<thead>
<tr>
<th>Status</th>
<th>Plugin Family</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Authentication &amp; Session</td>
<td>4</td>
</tr>
<tr>
<td>Disabled</td>
<td>Code Execution</td>
<td>5</td>
</tr>
<tr>
<td>Disabled</td>
<td>Cross Site Request Forgery</td>
<td>1</td>
</tr>
<tr>
<td>Disabled</td>
<td>Cross Site Scripting</td>
<td>8</td>
</tr>
<tr>
<td>Disabled</td>
<td>Data Exposure</td>
<td>7</td>
</tr>
<tr>
<td>Disabled</td>
<td>File Inclusion</td>
<td>2</td>
</tr>
<tr>
<td>Disabled</td>
<td>Injection</td>
<td>8</td>
</tr>
<tr>
<td>Disabled</td>
<td>Web Applications</td>
<td>19</td>
</tr>
<tr>
<td>Disabled</td>
<td>Web Servers</td>
<td>9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>Plugin Name</th>
<th>Plugin ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Access restriction bypass via origin spoof</td>
<td>98099</td>
</tr>
<tr>
<td>Disabled</td>
<td>Password field with auto-complete</td>
<td>98081</td>
</tr>
<tr>
<td>Disabled</td>
<td>Session fixation</td>
<td>98102</td>
</tr>
<tr>
<td>Disabled</td>
<td>Unencrypted password form</td>
<td>98082</td>
</tr>
</tbody>
</table>
Tip: You can search for plugins and plugin families using the Search Plugin Families box in the upper right corner.

9. Click **Save**.

The scan saves.
WAS Chrome Extension (Classic Interface)

You can use the Tenable.io Web Application Scanning Google Chrome extension to streamline web application scanning.

Before you begin:

- Download the Tenable.io Web Application Scanning Chrome Extension from the [Chrome Web Store](https://chrome.google.com/webstore/detail/tenableio-web-app-scan/aohjmkfojdichbblgilhaccbpmbojilj).
- Log in to Tenable.io, as described in [Log in to Tenable.io](https://tenable.com/support/guides/log-in-to-tenable).

To use the Tenable.io Web Application Scanning Chrome Extension:

1. In your browser, click the Tenable.io logo.

   ![Tenable.io extension window](image)

   The Tenable.io extension window appears.
2. Do one of the following:
• To create a new scan, click **New Scan**.

![New Scan Form](image)

1. From the **Select Folder** drop-down box, select the folder to which you want to save the scan.
2. In the **Name** box, type a name for the scan.
3. In the **URL** box, type the URL that you want to scan.
4. Click **Next**.
e. Click **Record**.

Click the record button to start your recording.

Wikipedia: http://wikipedia.com

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>TARGET</th>
<th>VALUE</th>
<th>EDIT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No data was found

Google Chrome opens the URL you specified.

f. Perform the login sequence you want to record.

A **Tenable.io is recording** message appears in the lower-right corner of the browser.

![Tenable.io is recording](image)

**Tenable.io is recording**

Click 'Done' to return to the recording extension.

<table>
<thead>
<tr>
<th>Record</th>
<th>Play</th>
<th>No Delay</th>
<th>Delete All</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Optional)*

h. Do one of the following:

- To play the recording, click **Play**.
- To add a delay between each action in the recording, click **No Delay**.
The button changes to **3s Delay**, **5s Delay**, and so on. Click the button until you reach the desired delay between actions.

- To delete the recording, click **Delete All**.
  
i. Click **Save**.

    ![Recording interface with commands]

    j. In your browser, highlight a section of text that is only shown when the login is successful.
Now that you are logged in please highlight a section of the text that is only shown when the login is successful.

Wikipedia

/From Wikipedia, the free encyclopedia/

The text appears in the plugin window.

**Tip:** Click the text block to edit the text.

k. Click **Done**.

A **Scan Updated** message appears.
l. Click **Access your updated scan here** to view the scan in Tenable.io.

- To add to an existing scan, click **Add to Existing Scan**:
  a. In the **Search** box, search for the scan to which you want to add.
  b. In the **Results** list, select the appropriate scan.

![Add to Existing Scan](image)

Search and then select an existing WAS Scan.

- **Search**

<table>
<thead>
<tr>
<th>3 records</th>
</tr>
</thead>
</table>

- **Results**

  ![Wikipedia]

  - **Wikipedia**

  ![Record](image)

  Click the record button to start your recording.

  **Wikipedia**: http://wikipedia.com

  ![No data was found](image)
Google Chrome opens the URL you previously specified.

e. Perform the login sequence you want to record. A **Tenable.io is recording** message appears in the lower-right corner of the browser.

```
Tenable.io is recording
Click 'Done' to return to the recording extension.
```

f. Click **Done**.

You return to the Tenable.io extension window.

g. (Optional) Do one of the following:

- To play the recording, click **Play**.
- To add a delay between each action in the recording, click **No Delay**. The button changes to **3s Delay**, **5s Delay**, and so on. Click the button until you reach the desired delay between actions.
- To delete the recording, click **Delete All**.
h. Click **Save**.

```
We recommend playing your scan before saving.

Wikipedia: http://wikipedia.com

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>TARGET</th>
<th>VALUE</th>
<th>EDIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. open</td>
<td><a href="https://www.wiki">https://www.wiki</a>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. setWindowSize</td>
<td>1680x947</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. type</td>
<td>css=#searchInput</td>
<td>Test</td>
<td></td>
</tr>
<tr>
<td>4. click</td>
<td>css=.pure-button</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

i. In your browser, highlight a section of text that is only shown when the login is successful.
Now that you are logged in please highlight a section of the text that is only shown when the login is successful.

Wikipedia

/From Wikipedia, the free encyclopedia/

The text appears in the plugin window.

Tip: Click the text block to edit the text.

j. Click Done.

A Scan Updated message appears.
k. Click **Access your updated scan here** to view the scan in Tenable.io.

**Note:** You can also access the Web Application Scanning Chrome Extension from the Scan Vulnerability information section. See View Vulnerability Information in the Tenable.io Vulnerability Management User Guide for more information.
Create an Agent Scan (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Note:** As a scan operator, you can only create a scan using user-defined policies that are shared with you.

To create an agent scan:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the upper right corner, click the **New Scan** button.
   
   The **Scan Templates** page appears.

3. Click the **Agent** tab.
   
   The **Agent** scan templates page appears.

4. Click the **scan template** that you want to use.
   
   **Tip:** Use the search box in the top navigation bar to filter templates on the tab currently in view.

5. Configure the scan’s **settings**.

6. (Optional) Configure **compliance checks** for the scan.

7. (Optional) Configure security checks by **plugin family or individual plugin**.

8. Do one of the following:
   
   - If you want to launch the scan later, click the **Save** button.
     
     Tenable.io saves the scan.
   
   - If you want to launch the scan immediately:
     
     a. Click the **button.

     b. Click **Launch**.

     Tenable.io saves and launches the scan.
Import a Scan (Classic Interface)

Required Tenable.io Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can import scan results into Tenable.io. You cannot import results from scans run more than 15 months ago.

Imported scans always belong to the default network. For more information, see Networks.

Note: Tenable.io supports scan imports up to 4GB in size.

To import a scan:

1. In the top navigation bar, click Scans.
   
   The My Scans page appears.

2. In the upper-right corner, click the Import button.
   
   Your browser’s file select window appears.

3. Go to and select the scan file that you want to import.
   
   If the scan file is a .nessus or .db file, the Import window appears.
   
   If the scan file is any other file type, the Scan Import window appears.

4. If the scan file is a .nessus or .db file, in the Password box, type the password to allow Tenable.io to view the scan.

5. (Optional) To show the scan results in dashboards, select the Show in Dashboard check box.
   
   Note: Clicking Cancel cancels the import.

6. Click Upload.
   
   The scan appears in the scans table.

   Tenable.io begins processing the imported scan results. Once this process is complete, the imported data appears in the individual scan details and aggregated data views (such as dashboards). This process can take up to 30 minutes, depending on the size of the import file.
Tip: If the imported data does not appear in the individual scan results or aggregated data views after a reasonable processing time, verify that you are assigned adequate permissions for the imported targets in access groups.
Launch a Scan (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can Control

In addition to configuring **Schedule** settings for a scan, you can manually start a scan run.

To launch a scan:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. (Optional) In the left navigation bar, click a different folder.

3. In the scans table, click the ▶ button next to the scan you want to launch.
   
   Tenable.io launches the scan.
Pause or Resume a Scan (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can Control

You can pause scans that you want to temporarily stop. When you pause a scan, Tenable.io pauses all active tasks for that scan. The paused tasks continue to fill the task capacity of the scanner that the tasks were assigned to. Tenable.io does not dispatch new tasks from a paused scan job. If the scan remains in a paused state for more than 14 days, the scan times out. Tenable.io terminates the related tasks on the scanner and categorizes the scan as aborted.

You can resume scans that you previously paused. When you resume a scan, Tenable.io instructs the scanner to start the tasks from the point at which the scan was paused. If Tenable.io encounters problems when resuming the scan, the scan fails, and Tenable.io categorizes the scan as aborted.

**To pause a scan:**

1. In the top navigation bar, click **Scans**.

   The **My Scans** page appears.

2. (Optional) In the left navigation bar, click a different folder.

3. In the scans table, next to a running scan, click the button to pause the scan.

   Tenable.io pauses the scan.

**To resume a scan:**

1. In the top navigation bar, click **Scans**.

   The **My Scans** page appears.

2. (Optional) In the left navigation bar, click a different folder.
3. In the scans table, next to a paused scan, click the ▶ button to resume the scan.

Tenable.io resumes the scan from the point at which it was paused.
Start or Stop a Scan (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can Control

To start a scan in the classic interface:

1. In the top navigation bar, click the **Scans** button.
   
   The **My Scans** page appears.

2. (Optional) If you want to select a scan from a different folder, on the left navigation bar, click the folder you want to access.
   
   A new scans page appears, displaying a scans table for the folder you selected.

3. In the scans table, on the row corresponding to the scan that you want to launch, click the ➤ button.
   
   Tenable.io launches the scan.

**Note:** When you run a scan, Tenable.io may take some time to complete the scan, depending on the system load. To avoid excessive scan times, schedule your scan launch times over a wide time period.

**Note:** If you schedule an excessive number of scans to run concurrently, you may exhaust the scanning capacity on Tenable.io. If necessary, Tenable.io staggers concurrent scans to ensure consistent scanning performance.

To stop a scan in the classic interface:

1. In the top navigation bar, click the **Scans** button.
   
   The **My Scans** page appears.
2. (Optional) If you want to select a scan from a different folder, on the left navigation bar, click the folder you want to access.

   A new scans page appears, displaying a scans table for the folder you selected.

3. In the scans table, on the row corresponding to the scan that you want to stop, click the button.

   A window appears, confirming your selection to stop the scan.

4. Click the **Stop** button.

   Tenable.io stops the scan.
View Scans (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can View

You can view configured and imported scans. If you have appropriate permissions, you can also perform actions to manage the scans.

Before you begin:

- [Create](#) or [import](#) one or more scans.

To view scans:

1. In the top navigation bar, click **Scans**.

   The **My Scans** page appears.

2. If the scan you want to move is not in the **My Scans** folder, in the left navigation bar, click the folder that contains the scan you want to move.

3. Do any of the following:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search box</td>
<td>Search the table by scan name.</td>
</tr>
<tr>
<td></td>
<td>In the top navigation bar:</td>
</tr>
<tr>
<td></td>
<td>a. In the <strong>Search Scans</strong> box, type a full or partial scan folder name.</td>
</tr>
<tr>
<td></td>
<td>b. Click the <strong>button</strong>.</td>
</tr>
<tr>
<td></td>
<td>Tenable.io filters the table to only those scans that match your search terms.</td>
</tr>
<tr>
<td>Scans table</td>
<td>• View summary information about each scan:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong> — The scan name.</td>
</tr>
</tbody>
</table>
• **Schedule** – The scan schedule.

• **Last Modified** – The date and time the scan was last modified.

• **View** scan results.

• **Export** scan results.

• **Edit** a scan configuration.

• **Copy** a scan configuration.

• **Move** a scan to the trash.

• **Move** a scan to a different folder.
Edit a Scan Configuration (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can Configure

To edit a scan configuration:

1. **View** your scans.
2. In the scans table, click the scan you want to edit.
   - The scan details appear.
3. In the upper-right corner of the page, click **Configure**.
   - The Scan Configuration page appears.
4. Configure the scan:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Settings</strong></td>
<td>Configure the settings for the template you chose. Settings include basic settings like scan name, targets, and scanner used, as well as more advanced settings you can use to refine the scan.</td>
</tr>
<tr>
<td><strong>Compliance/SCAP</strong></td>
<td>Specify which platforms you want to audit. Tenable, Inc. provides best practice audits for each platform. Additionally, you can upload a custom audit file.</td>
</tr>
<tr>
<td><strong>Plugins</strong></td>
<td>Select security checks by plugin family or individual plugin.</td>
</tr>
<tr>
<td><strong>Credentials</strong></td>
<td><strong>Note:</strong> Any credentials added to a scan (managed or scan-specific) override policy-specific credentials. Specify options to perform a credentialed scan:</td>
</tr>
<tr>
<td></td>
<td>• To add a managed credential, under Add Managed Cre-</td>
</tr>
</tbody>
</table>
To add a scan-specific credential (that is, a credential used only by this scan):

a. Under **Add Credentials**, click a credential type.

b. Configure the **credential settings**.

5. Click **Save** to save your changes to the scan.

Tenable.io saves the scan.
Change Scan Ownership (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

**Required Scan Permissions:** Owner

Before you begin:

- If the scan is based on a [policy](#), assign the new owner at least [Can View permissions](#) for that policy. Otherwise, the new owner cannot view the scan configuration.

**Note:** Only the scan owner can change scan ownership. Therefore, if an administrator needs to change the ownership of another user's scan, they must first [impersonate](#) the user account and then assign ownership to the appropriate user.

To change the ownership of a scan:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the scans table, click the row of the scan you want to modify.

   The results page for that scan appears. The active tab on this page depends on the status of the scan.

3. In the upper-right corner, click the **Configure** button.

   The **Settings** tab appears.

4. In the **Basic** section, click **Permissions**.

   The **Data Sharing** and **User Sharing** settings appear.

5. In the **User Sharing** section, in the **Owner** drop-down box, select a new user to assign ownership.

6. Click **Save**.

   Tenable assigns ownership to the selected user.
Update Scan Permissions (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Owner

In the Tenable.io classic interface, you can update the scan permissions for any scan.

To update scan permissions:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. (Optional) To view a different folder, in the left navigation bar, click the folder you want to view.

3. In the scans table, select the check box next to the scan you want to copy.

4. In the top navigation bar, click **More**.

5. Click **Permissions**.
   
   The **Update Permissions** window appears.

6. In the **Add users or groups** box, type the user or group with whom you want to share scan permissions.
   
   Tenable.io filters the list of users and groups based on your search criteria.

7. Select the user or user group with whom you want to share scan permissions.
   
   Tenable.io adds the user or group to the **Update Permissions** window.

8. Next to the user or group name, in the drop-down box, select the **user role permissions** that you want to assign to the user.

9. Click **Update**.
   
   Tenable.io applies the updated permissions to the scan.
Copy a Scan Configuration (Classic Interface)

Required Tenable.io Vulnerability Management User Role: Standard, Scan Manager, or Administrator

Required Tenable.io Web Application Scanning User Role: Scan Operator, Standard, Scan Manager, or Administrator

Required Scan Permissions: Owner

When you copy a scan configuration, Tenable.io assigns you owner permissions for the copy and assigns the copy scan permissions from the original scan.

To copy a scan configuration:

1. In the top navigation bar, click Scans.
   
   The My Scans page appears.

2. (Optional) In the left navigation bar, click a different folder.

3. In the scans table, select the check box next to the scan you want to copy.

4. In the top navigation bar, click More.

5. Click Copy to.
   
   A drop-down list of folders appears.

6. Select the folder where you want to save the copy.

   Tenable.io creates a copy of the scan with Copy of prepended to the name and assigns you owner permissions for the copy. The copy appears in the scans table of the folder you selected.
## Move a Scan to the Trash Folder (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can View

When you move a shared scan to the Trash folder, Tenable.io moves the scan for your account only. The scan remains in the original folder for all other users who have at least Can View permissions for the scan.

Scans moved to the Trash folder also appear in the All Scans folder, marked with the label, Trash.

**Note:** After you move a scan to the Trash folder, the scan remains in the Trash folder until a user with Can Configure permissions permanently deletes the scan.

To move a scan or scans to the Trash folder:

1. In the top navigation bar, click **Scans**.
   The My Scans page appears.

2. (Optional) In the left navigation bar, click a different folder.

3. Do one of the following:
   - To move a single scan to the trash, in the scans table, click the ✗ button next to the scan you want to move.
     Tenable.io moves the scan to the Trash folder.
   - To move multiple scans to the trash:
     a. Select the check box next to the scans you want to delete.
     b. In the upper-right corner, click **More**.
     c. Click **Delete**.
     Tenable.io moves the scan or scans you selected to the Trash folder.
Delete a Scan (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can Configure

When you permanently delete a scan, you delete the scan configuration and scan results for all users the scan is shared with.

**Before you begin:**

- Move the scan or scans you want to delete to the **Trash** folder.

**To permanently delete a scan or scans:**

1. In the top navigation bar, click **Scans**.
   The **My Scans** page appears.

2. Click the **Trash** folder in the left navigation bar.
   The **Trash** page appears.

3. Do one of the following:
   - To delete a scan, click the ✗ button next to the scan you want to permanently delete.
   - To delete multiple scans:
     a. Select the check box next to the scans you want to delete.
     b. In the upper-right corner, click **More**.
     c. Click **Delete**.

   • To delete all scans in the **Trash** folder, in the upper-right corner of the page, click **Empty Trash**.

   Tenable.io deletes the scan or scans you selected.
Delete Scan Job (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can Configure

When you delete a scan job, you delete only the scan results for a single instance of the scan being launched, known as a scan job. After you delete a scan job, you can launch the same scan. You can also still view the results from previous scan jobs run using the scan configuration.

To delete a scan job:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. (Optional) In the left navigation bar, click a different folder.

   **Note:** If your Tenable.io Web Application Scanning license expires, Tenable.io removes all your web application scans from the scans table.

3. In the scans table, click the scan for which you want to delete a scan job.

   The results page for that scan appears. The active tab on this page depends on the status of the scan.

4. Click the **History** tab.

   The **History** tab for the scan appears, displaying a table of each scan job for that scan.

5. Do one of the following:

   - To delete a single scan, in the history table, click the ✗ button next to the scan job you want to delete.
   - To delete multiple scan jobs:
a. Select the check box next to the scan jobs you want to delete.

b. In the upper-right corner, click **Delete**.

A **Delete History** window appears, asking you to confirm that you want to delete the scan job and the associated results.

6. Click **Delete**.

Tenable.io deletes the scan job.
## Tenable-Provided Scanner Templates (Classic Interface)

Templates facilitate the creation of **Scans** and **Policies**.

When you first create a **Scan** or **Policy**, the **Scan Templates** section or **Policy Templates** section appears, respectively. Templates are provided for scanners and agents. If you have created custom policies, they appear in the **User Defined** tab.

**Note:** If a plugin requires authentication or settings to communicate with another system, the plugin is not available on agents. This includes, but is not limited to:

- Patch management.
- Mobile device management.
- Cloud infrastructure audit.
- Database checks that require authentication.

Instead, use Tenable-provided **agent templates** for agent scanning.

The following tables list the templates that are available in Tenable.io and brief explanations of each template.

When you configure a Tenable-provided scan template, you can modify only the settings included for the scan template type. When you create a user-defined scan template, you can modify a custom set of settings for your scan.

For descriptions of all settings, see **Settings**.

### Scanner Templates

Scanner templates fall into three categories: **Discovery, Vulnerabilities**, and **Compliance**.

**Tip:** In the Tenable.io interface, use the search box to quickly find a template.

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Discovery</strong></td>
<td></td>
</tr>
<tr>
<td>Host Discovery</td>
<td>Performs a simple scan to discover live hosts and open ports.</td>
</tr>
<tr>
<td><strong>Vulnerabilities</strong></td>
<td></td>
</tr>
<tr>
<td>Template</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Advanced Network Scan</td>
<td>A scan without any recommendations, so that you can fully customize the scan settings.</td>
</tr>
<tr>
<td>Basic Network Scan</td>
<td>Performs a full system scan that is suitable for any host. For example, you could use this template to perform an internal vulnerability scan on your organization’s systems.</td>
</tr>
<tr>
<td></td>
<td><strong>Video:</strong> Launch a Basic Network Scan in Tenable.io</td>
</tr>
<tr>
<td>Badlock Detection</td>
<td>Performs remote and local checks for CVE-2016-2118 and CVE-2016-0128.</td>
</tr>
<tr>
<td>Bash Shellshock Detection</td>
<td>Performs remote and local checks for CVE-2014-6271 and CVE-2014-7169.</td>
</tr>
<tr>
<td>Credentialed Patch Audit</td>
<td>Authenticates hosts and enumerates missing updates.</td>
</tr>
<tr>
<td></td>
<td><strong>Video:</strong> Launch a Credentialed Scan in Tenable.io</td>
</tr>
<tr>
<td>DROWN Detection</td>
<td>Performs remote checks for CVE-2016-0800.</td>
</tr>
<tr>
<td>Malware Scan</td>
<td>Scans for malware on Windows and Unix systems.</td>
</tr>
<tr>
<td></td>
<td><strong>Video:</strong> Perform a Malware Scan in Tenable.io</td>
</tr>
<tr>
<td></td>
<td><strong>Video:</strong> Application, Malware, and Content Audits</td>
</tr>
<tr>
<td></td>
<td><strong>Video:</strong> Application, Malicious Software, and Content Audits</td>
</tr>
<tr>
<td>Mobile Device Scan</td>
<td>Assesses mobile devices via Microsoft Exchange or an MDM.</td>
</tr>
<tr>
<td>PrintNightmare</td>
<td>Performs local checks for CVE-2021-34527, the PrintNightmare Win-</td>
</tr>
<tr>
<td>Template</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>dows Print Spooler vulnerability.</td>
<td></td>
</tr>
<tr>
<td>Shadow Brokers Scan</td>
<td>Scans for vulnerabilities disclosed in the Shadow Brokers leaks.</td>
</tr>
<tr>
<td>WannaCry Ransomware</td>
<td>Scans for the WannaCry ransomware.</td>
</tr>
<tr>
<td>Zerologon Remote Scan</td>
<td>Detects Microsoft Netlogon elevation of privilege vulnerability (Zerologon).</td>
</tr>
<tr>
<td>Solorigate</td>
<td>Detects SolarWinds Solorigate vulnerabilities using remote and local checks.</td>
</tr>
<tr>
<td>Active Directory Starter Scan</td>
<td>Scans for misconfigurations in Active Directory.</td>
</tr>
<tr>
<td><strong>Note</strong>: Active Directory Starter Scans require ADSI credentials. For more information, see <a href="#">Miscellaneous</a>.</td>
<td></td>
</tr>
</tbody>
</table>

## Compliance

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Cloud Infrastructure</td>
<td>Audits the configuration of third-party cloud services.</td>
</tr>
<tr>
<td>Internal PCI Network Scan</td>
<td>Performs an internal PCI DSS (11.2.1) vulnerability scan.</td>
</tr>
<tr>
<td>MDM Config Audit</td>
<td>Audits the configuration of mobile device managers.</td>
</tr>
<tr>
<td>Offline Config Audit</td>
<td>Audits the configuration of network devices.</td>
</tr>
<tr>
<td>PCI Quarterly External Scan</td>
<td>Performs quarterly external scans as required by PCI.</td>
</tr>
<tr>
<td><strong>Note</strong>: Performs quarterly external scans as required by PCI.</td>
<td></td>
</tr>
<tr>
<td>Template</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Policy Compliance Auditing</td>
<td>Audits system configurations against a known baseline.</td>
</tr>
<tr>
<td>SCAP and OVAL Auditing</td>
<td>Audits systems using SCAP and OVAL definitions.</td>
</tr>
</tbody>
</table>

**Note:** Because the nature of a PCI ASV scan is more paranoid and may lead to false positives, the scan data is not included in the aggregate Tenable.io data. This is by design.

**Video:** [Launch a Compliance Scan in Tenable.io](#)
WAS Scan Templates (Classic Interface)

**Note:** This topic describes scan templates in the classic interface only. If you activate the new interface, you can use the classic interface to view a snapshot of historical scan templates you created and configured prior to activating the new interface. However, you can modify scan configurations in the new interface only.

When you activate the new interface, be aware of the following changes:

- In the new interface, the Legacy Web App Scan template appears in the Scanner tab.
- If you want to create or modify a scan or user-defined template based on the PCI WAS Scan template, you can use the classic interface only.

For a list of templates available in the new interface, see Scan Templates.

On the Scans page, the Web Application tab appears, displaying Tenable.io Web Application Scanning scan templates. You can use these templates with the default settings to create scans, or you can configure the templates based on your organization's web application scanning policies.

The Web Application tab displays the following Tenable.io Web Application Scanning scan type templates:

**Note:** Tenable recommends that you run a Web Application Overview scan the first time you scan a web application. After the scan completes, review the targeted URLs to determine whether scanning those URLs for vulnerabilities is sufficient. If scanning the target URLs is sufficient, use the default configurations when you run a Web App Scan. If not, configure the Web App Scan template settings to include or exclude certain URLs.

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web App Overview</td>
<td>High-level preliminary scan that determines which URLs in your web application that Tenable.io Web Application Scanning scans by default.</td>
</tr>
<tr>
<td>Web App Scan</td>
<td>Detailed scan that checks your web applications for vulnerabilities.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> A Web App Scan generally takes more time to complete than other Tenable scans.</td>
</tr>
<tr>
<td>Legacy Web App Scan</td>
<td>Detailed scan that allows you to use a Nessus scanner to scan your web applications.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Unlike the Tenable.io Web Application Scanning scanner, the Nessus scanner</td>
</tr>
</tbody>
</table>
does not use a browser to scan your web applications. Therefore, a Legacy Web App Scan is not as comprehensive as a Web App Scan.

| PCI WAS Scan       | A scan that assesses web applications for compliance to the Payment Card Industry Data Security Standards (PCI DSS) for PCI ASV. |

**Web App Overview Scan**

**Note:** To avoid an Access Denied error when running a scan, you must add an **Allow** rule to the Cloudflare firewall for the scan's user agent string.

**Basic Settings**

**General**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>None</td>
<td>The name of the scan or policy. This value appears in the Tenable.io interface.</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>None</td>
<td>A description of the scan or policy.</td>
<td>No</td>
</tr>
<tr>
<td>Folder</td>
<td>My Scans</td>
<td>The folder where the scan appears after saving.</td>
<td>No</td>
</tr>
<tr>
<td>Scanner</td>
<td>Varies</td>
<td>The scanner that performs the scan. The default scanner varies based on the organization and user.</td>
<td>No</td>
</tr>
<tr>
<td>Target</td>
<td>None</td>
<td>The target you want to scan, in URL format.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Schedule**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Off</td>
<td>Specifies whether the scan is scheduled. By default, scans are not scheduled.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Frequency</td>
<td>Once</td>
<td>How often the scan launches.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The frequency with which you scan your target depends on several factors (e.g., how often you update your web application, the content your web application contains, etc.). For most web applications, Tenable recommends at least monthly scans.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Once:</strong> Schedule the scan at a specific time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Daily:</strong> Schedule the scan to occur on a daily basis, at a specific time, for up to 20 days.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Weekly:</strong> Schedule the scan to occur on a recurring basis, by time and day of week, for up to 20 weeks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Monthly:</strong> Schedule the scan to occur every month, by time and day of month or week of month, for up to 20 months.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Yearly:</strong> Schedule the scan to occur every year, by time and day, for up to 20 years.</td>
</tr>
<tr>
<td>Starts</td>
<td>Varies</td>
<td>The exact date and time when a scan launches.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> If you schedule an excessive number of scans to run concurrently, you may exhaust the scanning capacity on Tenable.io Web Application Scanning. If necessary, Tenable.io Web Application Scanning staggers concurrent scans to ensure consistent scanning performance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The starting date defaults to the date when you create the scan. The starting time is the nearest next half-hour interval. For example, if you create your scan on October 31, 2016 at 9:12 AM, the default starting date and time is 10/31/2016 and 09:30.</td>
</tr>
<tr>
<td>Timezone</td>
<td>Zulu</td>
<td>The timezone of the value set for Starts.</td>
</tr>
<tr>
<td>Summary</td>
<td>Not applic-</td>
<td>A summary of the your scan’s schedule based on the val-</td>
</tr>
</tbody>
</table>
## Setting, Default Value, Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Able</td>
<td></td>
<td>Uses you specified for the available settings.</td>
</tr>
</tbody>
</table>

### Notifications

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Recipient(s)</td>
<td>None</td>
<td>The email addresses that Tenable.io Web Application Scanning alerts when a scan completes and results are available.</td>
</tr>
</tbody>
</table>

### Permissions

Using settings in the Permissions section, you can assign various permissions to groups and individual users. When you assign a permission to a group, that permission applies to all users within the group. The following rows describe the permissions that can be assigned.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Results</td>
<td>How scan results are displayed. You can select from the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Keep private</strong> - Tenable.io Web Application Scanning does not display the</td>
</tr>
<tr>
<td></td>
<td>results on the dashboard. Users with view, control, or configure permissions</td>
</tr>
<tr>
<td></td>
<td>can view the results only if the scan owner generates and shares a report</td>
</tr>
<tr>
<td></td>
<td>for the scan.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Show in dashboard</strong> - Tenable.io Web Application Scanning displays the</td>
</tr>
<tr>
<td></td>
<td>results on the dashboard.</td>
</tr>
<tr>
<td>Add users or</td>
<td>Which users or groups have access to the scan. When you give a user or group</td>
</tr>
<tr>
<td>groups</td>
<td>access, you can select from the following permissions:</td>
</tr>
<tr>
<td></td>
<td>• <strong>No Access</strong> - User or group cannot interact with the scan in any way.</td>
</tr>
<tr>
<td></td>
<td>When you create a scan or policy, no other users or groups have access to</td>
</tr>
<tr>
<td></td>
<td>it by default.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Can view</strong> - Can view scan results</td>
</tr>
</tbody>
</table>
## Setting Description

- **Can control** - Can view scan results and can also launch, pause, and stop a scan
- **Can configure** - Can modify the scan configurations and has all other user permissions previously mentioned

**Note:** When you apply a permission to a group, the permission applies to all users within the group. The following rows describe the permissions that you can assign.

### Scope Settings

The **Scope** settings specify URLs and file types that you want to include or exclude from your scan.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Inclusion</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List of URLs</td>
<td>None</td>
<td>A text box where you can type URLs to include in the scan.</td>
</tr>
<tr>
<td>Specify how the scanner handles URLs found during the application crawl</td>
<td>Cleared</td>
<td>This check box setting has three options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Crawl all URLs detected</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Limit crawling to specified URLs and child paths</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Limit crawling to specified URLs</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> To increase your scan's coverage and effectiveness, Tenable recommends that you first run an <strong>Overview</strong> scan and review the output for the <a href="https://tenable.com/docs/">Web Application Sitemap plugin</a>. Then, determine how to modify your configurations to refine the scope and eliminate redundant web pages.</td>
</tr>
<tr>
<td><strong>Scan Exclusion</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regex for excluded URLs</td>
<td>logout</td>
<td>A text box where you can specify the in-scope URL regex values to exclude from the scan. For example, if you type &quot;logout&quot;, any in-scope URL that includes the word &quot;logout&quot;</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>File extensions to exclude</td>
<td>css, js, png, jpeg, gif, pdf, csv</td>
<td>A text box in which you can type file types to exclude from the scan.</td>
</tr>
</tbody>
</table>

Discovery Settings

The **Discovery** settings include configurable settings that allow the scan to discover new URLs other than the ones discovered during crawling.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL Parameter Manipulation</td>
<td>Cleared</td>
<td>Whether the scanner will change values found in a query string, and resubmits the URL to discover new pages.</td>
</tr>
<tr>
<td>Maximum Manipulation Attempts</td>
<td>10</td>
<td>The maximum number of times the scanner will attempt to manipulate query string values.</td>
</tr>
<tr>
<td>Crawl Scripts</td>
<td>None</td>
<td>A link to upload one or more Selenium scripts to crawl during the scan.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To create a Selenium script, see the Selenium instructions in <a href="#">Web App Authentication</a>.</td>
</tr>
</tbody>
</table>

Advanced Settings

The **Advanced** settings provide increased control over scan efficiency and the operations of a scan, as well as the ability to enable plugin debugging.

General
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overall Scan max time (HH:MM:SS)</td>
<td>08:00:00</td>
<td>The maximum duration the scan runs before it stops automatically.</td>
</tr>
<tr>
<td><strong>Note</strong>: The maximum duration you can set</td>
<td></td>
<td></td>
</tr>
<tr>
<td>for your overall scan max time is 99:59:59</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(hours: minutes: seconds).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Debug logging for this scan</td>
<td>Off</td>
<td>A check box that, when selected, adds additional information to the scan's</td>
</tr>
<tr>
<td><strong>Note</strong>: Tenable recommends that you leave</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the setting off unless Tenable Support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>instructs you to enable it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Limits</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of URLs to Crawl and Browse</td>
<td>10000</td>
<td>The maximum number of URLs the scanner attempts to crawl and, therefore,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>audit.</td>
</tr>
<tr>
<td>Path Directory Depth</td>
<td>10</td>
<td>The maximum number of sub-directories the scanner crawls.</td>
</tr>
<tr>
<td>Page DOM Element Depth</td>
<td>5</td>
<td>The maximum depth of HTML nested elements the scanner crawls.</td>
</tr>
<tr>
<td>Maximum Response Size</td>
<td>500000</td>
<td>The maximum load size of a page in order to be audited.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the scanner crawls a URL and the response exceeds the limit, then it is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>not audited and no vulnerability assessment is performed.</td>
</tr>
<tr>
<td>Request Redirect Limit</td>
<td>1</td>
<td>The number of redirects the scan follows before it stops trying to crawl</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the page.</td>
</tr>
</tbody>
</table>

**Discovery**
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Crawl Settings</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| User Agent                    | WAS/%v        | The user-agent header used by the scanner when sending an HTTP request.  
**Note:** The %v placeholder indicates the version of the scan engine.                                                                                   |
| Custom Headers                | None          | A list of custom headers you want to inject into each HTTP request.  
**Note:** If you specify the user-agent value in this list, that value will override the value entered in the User Agent box.                               |
| **Screen Settings**           |               | settings of the virtual browser instance spun up by the scanner                                                                                       |
| Screen Width                  | 1600          | The screen width, in pixels, of the browser embedded into the scanner.                                                                                                                                   |
| Screen Height                 | 1200          | The screen height, in pixels, of the browser embedded into the scanner.                                                                                                                                   |
| Ignore Images                 | Selected      | Whether images on web pages should be crawled or ignored by the browser embedded into the scanner.                                                                                                         |
| **Selenium Settings**         |               |                                                                                                                                                            |
| Page rendering delay          | 10000         | The time, in milliseconds, to allow the browser to render the page.                                                                                                                                       |
| Command execution delay       | 500           | The time, in milliseconds, to wait after processing a command before processing a new one.                                                                                                                |
| Script completion delay       | 5000          | The time, in milliseconds, to wait once all commands are processed for rendering new content.                                                                                                            |

**Performance**
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max number of concurrent HTTP connections</td>
<td>10</td>
<td>The maximum number of established HTTP sessions for a single host.</td>
</tr>
<tr>
<td>Max number of HTTP requests per second</td>
<td>25</td>
<td>The maximum number of HTTP requests for the entire scan for a single host.</td>
</tr>
<tr>
<td>Slow down the scan when network congestion is detected</td>
<td>Selected</td>
<td>Whether the scan is throttled when it detects network congestion.</td>
</tr>
<tr>
<td>Network timeout (in seconds)</td>
<td>5</td>
<td>The time that the scanner waits for a response from a host, unless otherwise specified within a plugin. If you are scanning over a slow connection, you may wish to set this to a higher number of seconds.</td>
</tr>
<tr>
<td>Browser timeout (in seconds)</td>
<td>10</td>
<td>The time that the scanner waits for a response from a browser, unless otherwise specified within a plugin. If you are scanning over a slow connection, you may wish to set this to a higher number of seconds.</td>
</tr>
<tr>
<td>Timeout threshold</td>
<td>100</td>
<td>The number of consecutive timeouts before the scan aborts (minimum 100).</td>
</tr>
</tbody>
</table>

**Plugins**

You can enable or disable individual plugins and/or plugin families to customize your scan. When you click on a plugin, the following details appear:

- **Description**: A description of the discovered vulnerability.
- **Solution**: The steps that you can take to mitigate the discovered vulnerability.
- **Plugin Information**: The Plugin ID, publication date, and last modified date.
- **Risk Information**: The risk factor of the discovered vulnerability.
• **Reference Information:** The Open Web Application Security Project (OWASP) Top 10 number and the Web Application Security Consortium (WASC) classification.

**Credentials**

The **Web App Overview** scan template offers the following authentication methods:

- **HTTP Server Authentication:** authenticates toward the server.
- **Web Application Authentication - Login Form:** authenticates toward the application.
- **Web Application Authentication - Cookie Authentication:** authenticates toward the session.

**Note:** If the scan fails to authenticate, it aborts immediately with a message explaining that it could not authenticate.

**HTTP Server Authentication**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>None</td>
<td>The user name of the authorized user. For example, the user name of one of the users listed in the <code>httpasswd</code> file on an Apache server.</td>
</tr>
<tr>
<td>Password</td>
<td>None</td>
<td>The password of the authorized user.</td>
</tr>
</tbody>
</table>

**Web Application Authentication**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Method</td>
<td>Login Form</td>
<td>A box where you can specify one of two options: <strong>Login Form</strong> or <strong>Cookie Authentication</strong>. Depending on which option you select, the following options will appear:</td>
</tr>
<tr>
<td>Login Form</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Login Page</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Credentials</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
|                               |               | • Pattern to verify successful auth  
|                               |               | • Page to verify active session  
|                               |               | • Pattern to verify active session  
| **Cookie Authentication**     |               | **Note:** This parameter accepts relative or absolute URLs.  
|                               |               | **Note:** The form may require more than just the user name and password parameters, so you must provide all parameters required by the form to ensure proper authentication.  
| Login Page                    | None          | The URL that is specified in the form action attribute and used to submit the form authentication. This may not be the URL for the login form.  
|                               |               | **Note:** This parameter accepts relative or absolute URLs.  
| Credentials                   | None          | One or more key value pairs to perform authentication. The pairs are concatenated upon submission to create the list of parameters required by the form.  
|                               |               | For instructions on how to retrieve the key value pairs, see Configure WAS Login Form Authentication (Classic Interface).  
| Pattern to verify successful auth | None          | The regular expression to be matched against the form submission response to verify that the login was successful.  
| Session Cookies               | None          | One or more key value pairs to perform authentication. The pairs are concatenated upon submission to create the list of parameters required by the form.
Setting	Default Value	Description

of parameters required by the form.

For instructions on how to retrieve the key value pairs, see WAS Cookie Authentication (Classic Interface).

**Note:** The form may require more than just the user name and password parameters, so you must provide all parameters required by the form to ensure proper authentication.

Global Credential Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page to verify active session</td>
<td>None</td>
<td>The URL used to verify if the scan is authenticated.</td>
</tr>
<tr>
<td>Pattern to verify active session</td>
<td>None</td>
<td>The regular expression to be matched against the contents of the URL specified by the Page to verify active session parameter to verify if the scan is authenticated.</td>
</tr>
</tbody>
</table>

Web App Scan Settings

Basic Settings

General

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>None</td>
<td>The name of the scan or policy. This value appears in the Tenable.io interface.</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>None</td>
<td>A description of the scan or policy.</td>
<td>No</td>
</tr>
<tr>
<td>Folder</td>
<td>My Scans</td>
<td>The folder where the scan appears after saving.</td>
<td>Yes</td>
</tr>
<tr>
<td>Scanner</td>
<td>Varies</td>
<td>The scanner that performs the scan. The default scanner varies based on the organ-</td>
<td>Yes</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>---------</td>
<td>---------------</td>
<td>-----------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Target</td>
<td>None</td>
<td>The target you want to scan, in URL format.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Schedule

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Off</td>
<td>The toggle that specifies whether the scan is scheduled. By default, scans are not scheduled. To modify the following Schedule settings, click the Off button.</td>
</tr>
<tr>
<td>Frequency</td>
<td>Once</td>
<td>How often the scan launches.</td>
</tr>
</tbody>
</table>

**Note:** The frequency with which you scan your target depends on several factors (e.g., how often you update your web application, the content your web application contains, etc.). For most web applications, Tenable recommends at least monthly scans.

- **Once:** Schedule the scan at a specific time.
- **Daily:** Schedule the scan to occur on a daily basis, at a specific time, for up to 20 days.
- **Weekly:** Schedule the scan to occur on a recurring basis, by time and day of week, for up to 20 weeks.
- **Monthly:** Schedule the scan to occur every month, by time and day of month or week of month, for up to 20 months.
- **Yearly:** Schedule the scan to occur every year, by time and day, for up to 20 years.

| Starts  | Varies      | The exact date and time when a scan launches.                             |

**Note:** If you schedule an excessive number of scans to run con-
Currently, you may exhaust the scanning capacity on Tenable.io Web Application Scanning. If necessary, Tenable.io Web Application Scanning staggers concurrent scans to ensure consistent scanning performance.

The starting date defaults to the date when you create the scan. The starting time is the nearest next half-hour interval. For example, if you create your scan on 10/31/2016 at 9:12 AM, the default starting date and time is 10/31/2016 and 09:30.

Timezone | Zulu | The timezone of the value set for Starts.
Summary | Not applicable | A summary of the schedule for your scan based on the values you have specified for the available settings.

Notifications

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| Email Recipient(s)       | None          | The email addresses that are alerted when a scan completes and the results are available.

Permissions

Using settings in the Permissions section, you can assign various permissions to groups and individual users. When you assign a permission to a group, that permission applies to all users within the group. The following rows describe the permissions that can be assigned.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add users or groups</td>
<td>The users or groups to which you want to apply permissions.</td>
</tr>
</tbody>
</table>

Note: When you apply a permission to a group, the permission applies to all users within the group. The following rows describe the permissions that you can assign.
Setting | Description
--- | ---
No access | Groups and users set to **No access** cannot interact with the scan in any way. When you create a scan or policy, no other users or groups have access to it by default.
Can view | Groups and users set to **Can view** can view the results of the scan.
Can control | Groups and users set to **Can control** can launch, pause, and stop a scan, as well as view its results.
Can configure | Groups and users set to **Can configure** can modify the configuration of the scan in addition to all other permissions.

**Scope Settings**

The **Scope** settings specify URLs and file types that you want to include or exclude from your scan.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Inclusion</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List of URLs</td>
<td>None</td>
<td>A text box in which you can type URLs to include in the scan.</td>
</tr>
</tbody>
</table>
| Specify how the scanner handles URL’s found during the application crawl | Cleared | This setting has three options:  
- **Crawl all URLs detected**  
- **Limit crawling to specified URLs and child paths**  
- **Limit crawling to specified URLs**  |

**Note:** To increase your scan’s coverage and effectiveness, Tenable recommends that you first run an **Overview** scan and review the output for the **Web Application Sitemap plugin**. Then, determine how to modify your configurations to refine the scope and eliminate redundant web pages.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Exclusion</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Setting | Default Value | Description
--- | --- | ---
Regex for excluded URLs | logout | A text box in which you can specify in-scope URL regex values to exclude from the scan. For example, if you type "logout", then any in-scope URL that includes the word "logout" is excluded.

File extensions to exclude | css, js, png, jpeg, gif, pdf, csv | A text box in which you can type file types to exclude from the scan.

### Discovery Settings
The **Discovery** settings include configurable settings that allow the scan to discover new URLs other than the ones discovered during crawling.

| Setting | Default Value | Description |
--- | --- | ---
URL Parameter Manipulation | Cleared | Whether the scanner will change values found in a query string, and resubmits the URL to discover new pages. |
Maximum Manipulation Attempts | 10 | The maximum number of times the scanner will attempt to manipulate query string values. |
Crawl Scripts | None | A link to upload one or more Selenium scripts to crawl during the scan. To create a Selenium script, see the **To create a script to log in with your credentials** instructions on Configure Selenium Authentication. |

### Assessment Settings
The **Assessment** settings include configurable settings that allow the scan to audit elements other than the ones discovered during crawling. If you select **Custom** in the **Scan Type** drop-down box, the **General** section appears.
**Note:** When you select a check box for an option in the **Elements** section, the scanner analyzes that element type and tests all instances of the element for security vulnerabilities (e.g., OWASP Top 10).

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Elements</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit cookies</td>
<td>Selected</td>
<td>The scan checks for cookie-based vulnerabilities.</td>
</tr>
<tr>
<td>Audit forms</td>
<td>Selected</td>
<td>The scan checks for form-based vulnerabilities.</td>
</tr>
<tr>
<td>Audit headers</td>
<td>Selected</td>
<td>The scan inspects headers for vulnerabilities and insecure configurations (e.g., missing X-Frame-Options).</td>
</tr>
<tr>
<td>Audit links</td>
<td>Selected</td>
<td>The scan includes links and their parameters in vulnerability checks.</td>
</tr>
<tr>
<td>Audit parameter names</td>
<td>Cleared</td>
<td>The scan performs extensive fuzzing of parameter names.</td>
</tr>
<tr>
<td>Audit parameter values</td>
<td>Selected</td>
<td>The scan performs extensive fuzzing of parameter values.</td>
</tr>
<tr>
<td>Audit JSON</td>
<td>Cleared</td>
<td>The scan audits JSON request data.</td>
</tr>
<tr>
<td>Audit XML</td>
<td>Cleared</td>
<td>The scan audits XML request data.</td>
</tr>
<tr>
<td>Audit UI Forms</td>
<td>Selected</td>
<td>The scan checks input and button groups associated with JavaScript code.</td>
</tr>
<tr>
<td>Audit UI Inputs</td>
<td>Selected</td>
<td>The scan checks orphan input elements with associated DOM events.</td>
</tr>
<tr>
<td><strong>Options</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL for Remote File</td>
<td><a href="http://rfi.nessus.org/rfi.txt">http://rfi.nessus.org/rfi.txt</a></td>
<td>During Remote File Inclusion (RFI) testing, this setting specifies a file on a remote host to</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Inclusion use for tests. By default, Tenable.io uses a safe file hosted by Tenable for RFI testing. If the scanner cannot reach the Internet, you can use an internally hosted file for more accurate RFI testing.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Advanced Settings**

The **Advanced** settings provide increased control over scan efficiency and the operations of a scan, as well as the ability to enable plugin debugging.

**General**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overall Scan max time (HH:MM:SS)</td>
<td>08:00:00</td>
<td>The maximum duration the scan runs before it stops automatically.</td>
</tr>
<tr>
<td><strong>Note</strong>: The maximum duration you can set for your overall scan max time is 99:59:59 (hours: minutes: seconds).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Debug logging for this scan</td>
<td>Off</td>
<td>A check box that, when selected, adds additional information to the scan's log to assist with debugging.</td>
</tr>
<tr>
<td><strong>Note</strong>: Tenable recommends that you leave this setting off unless Tenable Support instructs you to enable it.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Limits</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of URLs to Crawl and Browse</td>
<td>10000</td>
<td>The maximum number of URLs the scanner attempts to crawl and therefore audit.</td>
</tr>
<tr>
<td>Path Directory</td>
<td>10</td>
<td>The maximum number of sub-directories the scanner</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Depth</td>
<td></td>
<td>Crawls.</td>
</tr>
<tr>
<td>Page DOM Element Depth</td>
<td>5</td>
<td>The maximum depth of HTML nested elements the scanner crawls.</td>
</tr>
<tr>
<td>Maximum Response Size</td>
<td>500000</td>
<td>The maximum load size of a page in order to be audited. If the scanner crawls a URL and the response exceeds the limit, then it is not audited and no vulnerability assessment is performed.</td>
</tr>
<tr>
<td>Request Redirect Limit</td>
<td>1</td>
<td>The number of redirects the scan follows before it stops trying to crawl the page.</td>
</tr>
</tbody>
</table>

### Discovery

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crawl Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Agent</td>
<td>WAS/%v</td>
<td>The user-agent header used by the scanner when sending an HTTP request.</td>
</tr>
<tr>
<td>Note: The %v placeholder indicates the version of the scan engine.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom Headers</td>
<td>None</td>
<td>A list of custom headers you want to inject into each HTTP request.</td>
</tr>
<tr>
<td>Note: If you specify the user-agent value in this list, that value will override the value entered in the User Agent box.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Screen Settings - settings of the virtual browser instance spun up by the scanner</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Screen Width</td>
<td>1600</td>
<td>The screen width, in pixels, of the browser embedded into the scanner.</td>
</tr>
</tbody>
</table>
## Setting

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screen Height</td>
<td>1200</td>
<td>The screen height, in pixels, of the browser embedded into the scanner.</td>
</tr>
<tr>
<td>Ignore Images</td>
<td>Selected</td>
<td>Whether images on web pages should be crawled or ignored by the browser embedded into the scanner.</td>
</tr>
</tbody>
</table>

## Performance

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max number of concurrent HTTP connections</td>
<td>10</td>
<td>The maximum number of established HTTP sessions for a single host.</td>
</tr>
<tr>
<td>Max number of HTTP requests per second</td>
<td>25</td>
<td>The maximum number of HTTP requests for the entire scan for a single host.</td>
</tr>
<tr>
<td>Slow down the scan when network congestion is detected</td>
<td>Selected</td>
<td>Whether the scan will be throttled when network congestion is detected.</td>
</tr>
<tr>
<td>Network timeout (in seconds)</td>
<td>5</td>
<td>The time that the scanner waits for a response from a host, unless otherwise specified within a plugin. If you are scanning over a slow connection, you may wish to set this to a higher number of seconds.</td>
</tr>
<tr>
<td>Browser timeout (in seconds)</td>
<td>10</td>
<td>The time that the scanner waits for a response from a browser, unless otherwise specified within a plugin. If you are scanning over a slow connection, you may wish to set this to a higher number of seconds.</td>
</tr>
<tr>
<td>Timeout threshold</td>
<td>100</td>
<td>The number of consecutive timeouts before the scan is aborted (minimum 100).</td>
</tr>
</tbody>
</table>
Plugins

You can enable or disable individual plugins and/or plugin families to customize your scan. When you click on a plugin, the following details appear:

- **Description**: A description of the discovered vulnerability.
- **Solution**: The steps that you can take to mitigate the discovered vulnerability.
- **Plugin Information**: The Plugin ID, publication date, and last modified date.
- **Risk Information**: The risk factor of the discovered vulnerability.
- **Reference Information**: The Open Web Application Security Project (OWASP) Top 10 number, the Common Weakness Enumeration (CWE) number, and the Web Application Security Consortium (WASC) classification, as applicable.

Credentials

The **Web App Scan** scan template offers three different authentication methods:

- **HTTP Server Authentication**: authenticates toward the server.
- **Web Application Authentication - Login Form**: authenticates toward the application.
- **Web Application Authentication - Cookie Authentication**: authenticates toward the session.

**Note**: If the scan fails to authenticate, it aborts immediately with a message explaining that it could not authenticate.

HTTP Server Authentication

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>None</td>
<td>The user name of the authorized user. For example, the user name of one of the users listed in the <strong>htpasswd</strong> file on an Apache server.</td>
</tr>
<tr>
<td>Password</td>
<td>None</td>
<td>The password of the authorized user.</td>
</tr>
</tbody>
</table>

Web Application Authentication
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td></td>
<td>Allows you specify whether you want to use a login form or cookie authentication to authenticate the scan.</td>
</tr>
<tr>
<td>Method</td>
<td>Login Form</td>
<td>Depending on which option you select, the following options will appear:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Login Form</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Login Page</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Credentials</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Pattern to verify successful auth</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Page to verify active session</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Pattern to verify active session</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Cookie Authentication</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Session Cookies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Page to verify active session</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Pattern to verify active session</td>
</tr>
<tr>
<td>Login Page</td>
<td>None</td>
<td>The URL that is specified in the <em>form action</em> attribute and used to submit the form authentication. This may not be the URL for the login form.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> This parameter accepts relative or absolute URLs.</td>
</tr>
<tr>
<td>Credentials</td>
<td>None</td>
<td>One or more key value pairs to perform authentication. The pairs are concatenated upon submission to create the list of parameters required by the form.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For instructions on how to retrieve the key value pairs, see Configure WAS Login Form Authentication (Classic Inter-</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Pattern to verify</td>
<td>None</td>
<td>The regular expression to be matched against the form submission response to verify that the login was successful.</td>
</tr>
<tr>
<td>successful auth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session Cookies</td>
<td>None</td>
<td>One or more key value pairs to perform authentication. The pairs are concatenated upon submission to create the list of parameters required by the form.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global Credential</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Page to verify active</td>
<td>None</td>
<td>The URL used to verify if the scan is authenticated.</td>
</tr>
<tr>
<td>session</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pattern to verify</td>
<td>None</td>
<td>The regular expression to be matched against the contents of the URL specified by the Page to verify active session parameter to verify if the scan is authenticated.</td>
</tr>
<tr>
<td>active session</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Legacy Web App Scan Settings**

**Basic Settings**

**General**
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>None</td>
<td>The name of the scan or policy. This value appears in the Tenable.io interface.</td>
</tr>
<tr>
<td>Description</td>
<td>None</td>
<td>A description of the scan or policy.</td>
</tr>
<tr>
<td>Folder</td>
<td>My Scans</td>
<td>The folder where the scan appears after being saved.</td>
</tr>
<tr>
<td>Scanner</td>
<td>Varies</td>
<td>The scanner that performs the scan. The default scanner varies based on the organization and user.</td>
</tr>
<tr>
<td>Target</td>
<td>None</td>
<td>The target you want to scan, in URL format.</td>
</tr>
<tr>
<td>Upload Targets</td>
<td>None</td>
<td>A link to upload a text file that specifies targets. The targets file must be formatted in the following manner:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The file must be ASCII format.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Only one target per line.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• No extra spaces should appear at the end of a line.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• No extra lines should appear following the last target.</td>
</tr>
<tr>
<td>Note:</td>
<td></td>
<td>Unicode/UTF-8 encoding is not supported.</td>
</tr>
</tbody>
</table>

**Schedule**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Off</td>
<td>The toggle that specifies whether the scan is scheduled. By default, scans are not scheduled. To modify the following Schedule settings, click the Off button.</td>
</tr>
<tr>
<td>Frequency</td>
<td>Once</td>
<td>How often the scan launches.</td>
</tr>
<tr>
<td>Note:</td>
<td></td>
<td>The frequency with which you scan your target depends on several factors (e.g., how often you update your web applic-</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For most web applications, Tenable recommends at least monthly scans.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Once</strong>: Schedule the scan at a specific time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Daily</strong>: Schedule the scan to occur on a daily basis, at a specific time, for up to 20 days.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Weekly</strong>: Schedule the scan to occur on a recurring basis, by time and day of week, for up to 20 weeks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Monthly</strong>: Schedule the scan to occur every month, by time and day of month or week of month, for up to 20 months.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Yearly</strong>: Schedule the scan to occur every year, by time and day, for up to 20 years.</td>
</tr>
<tr>
<td>Starts</td>
<td>Varies</td>
<td>The exact date and time when a scan launches.</td>
</tr>
<tr>
<td>Timezone</td>
<td>Zulu</td>
<td>The timezone of the value set for <strong>Starts</strong>.</td>
</tr>
<tr>
<td>Summary</td>
<td>Not applicable</td>
<td>A summary of the schedule for your scan based on the values you have specified for the available settings.</td>
</tr>
</tbody>
</table>

**Note**: If you schedule an excessive number of scans to run concurrently, you may exhaust the scanning capacity on Tenable.io Web Application Scanning. If necessary, Tenable.io Web Application Scanning staggers concurrent scans to ensure consistent scanning performance.

The starting date defaults to the date when you create the scan. The starting time is the nearest next half-hour interval. For example, if you create your scan on 10/31/2016 at 9:12 AM, the default starting date and time is **10/31/2016 and 09:30**.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Recipient(s)</td>
<td>None</td>
<td>The email addresses that are alerted when a scan completes and the results are available.</td>
</tr>
<tr>
<td>Result Filters</td>
<td>None</td>
<td>The type of information to be emailed.</td>
</tr>
</tbody>
</table>

**Permissions**

Using settings in the **Permissions** section, you can assign various permissions to groups and individual users. When you assign a permission to a group, that permission applies to all users within the group. The following rows describe the permissions that can be assigned.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Sharing</td>
<td></td>
</tr>
<tr>
<td>Scan results</td>
<td>Specifies whether you want scan results to be private to your user account, or appear in the <strong>Web Applications</strong> workbench.</td>
</tr>
<tr>
<td>User Sharing</td>
<td></td>
</tr>
<tr>
<td>Add users or groups</td>
<td>The users or groups to which you want to apply permissions.</td>
</tr>
<tr>
<td>Note:</td>
<td><strong>When you apply a permission to a group, the permission applies to all users within the group. The following rows describe the permissions that you can assign.</strong></td>
</tr>
<tr>
<td>No access</td>
<td>Groups and users set to <strong>No access</strong> cannot interact with the scan in any way. When you create a scan or policy, no other users or groups have access to it by default.</td>
</tr>
<tr>
<td>Can view</td>
<td>Groups and users set to <strong>Can view</strong> can view the results of the scan.</td>
</tr>
<tr>
<td>Can control</td>
<td>Groups and users set to <strong>Can control</strong> can launch, pause, and stop a scan, as well as view its results.</td>
</tr>
<tr>
<td>Can configure</td>
<td>Groups and users set to <strong>Can configure</strong> can modify the configuration of the scan in addition to all other permissions.</td>
</tr>
</tbody>
</table>

**Discovery Settings**
The **Discovery** settings include configurable settings that allow the scan to discover new URLs other than the ones discovered during crawling. If you select **Custom** in the **Scan Type** drop-down box, the **Host Discovery**, **Port Scanning**, and **Service Discovery** sections appear.

### Host Discovery

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping the remote host</td>
<td>On</td>
<td>This option enables Tenable.io Web Application Scanning to ping remote hosts on multiple ports to determine if the hosts are alive. When set to <strong>On</strong>, <strong>General Settings</strong> and <strong>Ping Methods</strong> appear.</td>
</tr>
</tbody>
</table>

**Note:** To scan VMware guest systems, **Ping the remote host** must be set to **Off**.

### General Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use fast network discovery</td>
<td>Cleared</td>
<td>If a host responds to ping, Tenable.io Web Application Scanning attempts to avoid false positives, performing additional tests to verify the response did not come from a proxy or load balancer. Selecting <strong>Use fast network discovery</strong> bypasses those additional tests.</td>
</tr>
</tbody>
</table>

### Ping Methods

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>Selected</td>
<td>Pings a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.</td>
</tr>
<tr>
<td>TCP</td>
<td>Selected</td>
<td>Pings a host using Transmission Control Protocol (TCP).</td>
</tr>
<tr>
<td>Destination ports (TCP)</td>
<td>built-in</td>
<td>Destination ports can be configured to use specific ports for TCP ping. This specifies the list of ports that are checked via TCP ping.</td>
</tr>
</tbody>
</table>
| ICMP                     | Selected      | Pings a host using the Internet Control Message Prot-
<table>
<thead>
<tr>
<th>Feature</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assume ICMP unreachable from the gateway</td>
<td>Cleared</td>
<td>When a ping is sent to a host that is down, its gateway may return an ICMP unreachable message. When you select <strong>Assume ICMP unreachable from the gateway means the host is down</strong>, when Tenable.io Web Application Scanning receives an ICMP Unreachable message, it considers the targeted host dead. This option helps speed up discovery on some networks.</td>
</tr>
<tr>
<td>Maximum number of retries</td>
<td>2</td>
<td>The number of attempts to retry pinging the remote host.</td>
</tr>
<tr>
<td>UDP</td>
<td>Cleared</td>
<td>Pings a host using the User Datagram Protocol (UDP). UDP is a stateless protocol, meaning that communication is not performed with handshake dialogues. UDP-based communication is not always reliable, and because of the nature of UDP services and screening devices, these services and devices are not always remotely detectable.</td>
</tr>
</tbody>
</table>

**Fragile Devices**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Network Printers</td>
<td>Cleared</td>
<td>Instructs Tenable.io Web Application Scanning to scan network printers.</td>
</tr>
<tr>
<td>Scan Novell NetWare hosts</td>
<td>Cleared</td>
<td>Instructs Tenable.io Web Application Scanning to scan Novell NetWare hosts.</td>
</tr>
</tbody>
</table>

**Wake-on-LAN (Local Area Network)**

The **Wake-on-LAN (WOL)** menu identifies the hosts to which you want to send WOL magic packets prior to running a scan.
### List of MAC addresses
None
You can provide hosts that you want to start prior to scanning by uploading a text file that lists one MAC address per line.

For example:

```
33:24:4C:03:CC:C7
FF:5C:2C:71:57:79
```

### Boot time wait (in minutes)
5
The amount of time to wait for hosts to start before performing the scan.

### Network Type

<table>
<thead>
<tr>
<th>Network Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mixed (use RFC 1918)</td>
<td>Specifies if you are using publicly routable IPs, private non-Internet routable IPs, or a mix of these.</td>
</tr>
</tbody>
</table>

This setting has three options:

- **Mixed (use RFC 1918)**
- **Private LAN**
- **Public WAN (Internet)**

The default value, **Mixed**, should be selected if you are using RFC 1918 addresses and have multiple routers within your network.

### Port Scanning

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consider unscanned ports as</td>
<td>Cleared</td>
<td>If a port is not scanned with a selected port scanner (for example, the port falls outside of the specified range), Tenable.io Web Application Scanning considers it closed.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>closed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port scan range</td>
<td>default</td>
<td>Two keywords can be typed into the Port scan range box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>default</em> instructs Tenable.io Web Application Scanning to scan approximately 4,790 commonly used ports. The list of ports can be found in the nessus-service file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>all</em> instructs Tenable.io Web Application Scanning to scan all 65,536 ports, including port 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Additionally, you can type a custom range of ports by using a comma-delimited list of ports or port ranges. For example, 21, 23, 25, 80, 110 or 1-1024, 8080, 9000-9200. If you wanted to scan all ports excluding port 0, you would type 1-65535.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The custom range specified for a port scan is applied to the protocols you selected in the Network Port Scanners group of settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If scanning both TCP and UDP, you can specify a split range specific to each protocol. For example, if you want to scan a different range of ports for TCP and UDP in the same policy, you would type T:1-1024, U:300-500.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can also specify a set of ports to scan for both protocols, as well as individual ranges for each separate protocol. For example, 1-1024, T:1024-65535, U:1025.</td>
</tr>
</tbody>
</table>

**Network Port Scanners**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>Cleared</td>
<td>On some platforms (e.g., Windows and Mac OS X), enabling this scanner causes Tenable.io Web Application Scanning to use the SYN scanner to avoid serious performance issues</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>native to those operating systems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Override automatic firewall detection</td>
<td>Cleared</td>
<td>When enabled, this setting overrides automatic firewall detection. This setting has three options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Use soft detection</strong> disables the ability to monitor how often resets are set and to determine if there is a limitation configured by a downstream network device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Use aggressive detection</strong> attempts to run plugins even if the port appears to be closed. Tenable, Inc. does not recommend that you select this option on a production network.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Disable detection</strong> disables the firewall detection feature. This description also applies to the <strong>Override automatic firewall detection</strong> setting that is available following SYN.</td>
</tr>
<tr>
<td>SYN</td>
<td>Selected</td>
<td>Use the Tenable.io Web Application Scanning SYN scanner to identify open TCP ports on the target hosts. SYN scans are generally considered to be less intrusive than TCP scans depending on the security monitoring device, such as a firewall or Intrusion Detection System (IDS). The scanner sends a SYN packet to the port, waits for SYN-ACK reply, and determines the port state based on a reply or lack of reply.</td>
</tr>
<tr>
<td>UDP</td>
<td>Cleared</td>
<td>This option enables the Tenable.io Web Application Scanning built-in UDP scanner to identify open UDP ports on the targets. Due to the nature of the protocol, it is generally not possible</td>
</tr>
</tbody>
</table>
Setting | Default Value | Description
--- | --- | ---
|  |  | for a port scanner to tell the difference between open and filtered UDP ports. Enabling the UDP port scanner may dramatically increase the scan time and produce unreliable results. Consider using the netstat or SNMP port enumeration options instead.

## Service Discovery

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Probe all ports to find services | Selected | Attempts to map each open port with the service that is running on that port.  
**Caution:** In some rare cases, probing might disrupt some services and cause unforeseen side effects. |
| Search for SSL/TLS services | On | Controls how Tenable.io Web Application Scanning will test Secure Sockets Layer (SSL)- and Transport Layer Security (TLS)-based services.  
**Caution:** Testing for SSL capability on all ports may be disruptive for the tested host. |
| Search for SSL/TLS on Known SSL/TLS ports |  | This setting has two options:  
- **Known SSL/TLS ports**  
- **All ports** |
| Identify certificates expiring within x days | 60 | Identifies SSL and TLS certificates that are within the specified number of days of expiring. |
### Setting

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enumerate all SSL/TLS ciphers</td>
<td>Selected</td>
<td>When enabled, Tenable.io Web Application Scanning ignores the list of ciphers advertised by SSL/TLS services and enumerates them by attempting to establish connections using all possible ciphers.</td>
</tr>
<tr>
<td>Enable CRL checking (connects to Internet)</td>
<td>Cleared</td>
<td>When enabled, Tenable.io Web Application Scanning checks that none of the identified certificates have been revoked.</td>
</tr>
</tbody>
</table>

### Assessment Settings

#### General

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Override normal accuracy</td>
<td>Cleared</td>
<td>In some cases, Tenable.io Web Application Scanning cannot remotely determine whether a flaw is present or not.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Show potential false alarms</strong>: A flaw is reported every time, even when there is a doubt about the remote host being affected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Avoid potential false alarms</strong>: Tenable.io Web Application Scanning will not report any flaw whenever there is a hint of uncertainty about the remote host.</td>
</tr>
<tr>
<td>Perform thorough tests (may disrupt your network or impact scan speed)</td>
<td>Cleared</td>
<td>When enabled, this option causes various plugins to work harder. For example, when looking through Server Message Block (SMB) file shares, a plugin can analyze 3 directory levels deep instead of 1. This could cause much more network traffic and analysis in some cases. By being more thorough, the scan is more intrusive and is more likely to disrupt the network, while potentially providing better audit results.</td>
</tr>
</tbody>
</table>

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
Web Applications

By default, web applications are not scanned. When you first access the Web Application section, the **Scan web applications** setting appears and is set to Off. To modify the Web Application settings listed on the following table, click the Off button. The rest of the settings appear.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use a custom User-Agent</td>
<td>Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)</td>
<td>Specifies which type of web browser Tenable.io Web Application Scanning impersonates while scanning.</td>
</tr>
<tr>
<td><strong>Web Crawler</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start crawling from</td>
<td>/</td>
<td>The URL of the first page that is tested. If multiple pages are required, use a colon delimiter to separate them (e.g., //:ph/p4:/base).</td>
</tr>
<tr>
<td>Excluded pages (regex)</td>
<td>/server_privileges.php</td>
<td>logout</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tenable.io Web Application Scanning supports POSIX regular expressions for string matching and handling, as well as Perl-Compatible Regular Expressions (PCRE).</td>
</tr>
<tr>
<td>Maximum pages to crawl</td>
<td>1000</td>
<td>The maximum number of pages to crawl.</td>
</tr>
<tr>
<td>Maximum depth to crawl</td>
<td>6</td>
<td>Limit the number of links Tenable.io Web Application Scanning follows for each start page.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Follow dynamically generated pages</td>
<td>Cleared</td>
<td>If selected, Tenable.io Web Application Scanning follows dynamic links and may exceed the parameters set in the <strong>Web Crawler</strong> section.</td>
</tr>
<tr>
<td><strong>Application Test Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable generic web application tests</td>
<td>Selected</td>
<td>Enables the options listed below.</td>
</tr>
<tr>
<td>Abort web application tests if HTTP login fails</td>
<td>Cleared</td>
<td>If Tenable.io Web Application Scanning cannot log in to the target via HTTP, then Tenable.io Web Application Scanning does not run any web application tests.</td>
</tr>
<tr>
<td>Try all HTTP methods</td>
<td>Cleared</td>
<td>This option instructs Tenable.io Web Application Scanning to also use POST requests for enhanced web form testing. By default, the web application tests only use GET requests, unless this option is enabled. Generally, more complex applications use the POST method when a user submits data to the application. When selected, Tenable.io Web Application Scanning tests each script or variable with both GET and POST requests. This setting provides more thorough testing, but may considerably increase the time required.</td>
</tr>
<tr>
<td>Attempt HTTP Parameter Pollution</td>
<td>Cleared</td>
<td>When performing web application tests, attempt to bypass filtering mechanisms by injecting content into a variable while also supplying the same variable with valid content.</td>
</tr>
</tbody>
</table>
### Setting | Default Value | Description
--- | --- | ---
| | | tent. For example, a normal SQL injection test may look like /target.cgi?a='&b=2. With HTTP Parameter Pollution (HPP) enabled, the request may look like /target.cgi?a='&a=1&b=2.

**Test embedded web servers** | Cleared | Embedded web servers are often static and contain no customizable CGI scripts. In addition, embedded web servers may be prone to crash or become non-responsive when scanned. Tenable recommends selecting this option to scan embedded web servers separately from other web servers.

**Test more than one parameter at a time perform** | Cleared | This setting manages the combination of argument values used in the HTTP requests. The default, without checking this option, is testing one parameter at a time with an attack string, without trying non-attack variations for additional parameters. For example, Tenable.io Web Application Scanning would attempt /test.php?arg1=XSS&b=1&c=1, where b and c allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated.

This setting has four options:

- **Test random pairs of parameters**: This form of testing randomly checks a combination of random pairs of parameters. This is the fastest way to test
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>multiple parameters.</td>
</tr>
<tr>
<td>• Test all pairs of parameters (slow):</td>
<td></td>
<td>This form of testing is slightly slower but more efficient than the one value test. While testing multiple parameters, it tests an attack string, variations for a single variable and then uses the first value for all other variables. For example, Tenable.io Web Application Scanning would attempt /test.php?a=XSS&amp;b=1&amp;c=1&amp;d=1 and then cycle through the variables so that one is given the attack string, one is cycled through all possible values (as discovered during the mirror process), and any other variables are given the first value. In this case, Tenable.io Web Application Scanning would never test for /test.php?a=a=XSS&amp;b=3&amp;c=3&amp;d=3 when the first value of each variable is 1.</td>
</tr>
<tr>
<td>• Test random combinations of three or more parameters (slower):</td>
<td></td>
<td>This form of testing randomly checks a combination of three or more parameters. This is more thorough than testing only pairs of parameters. Increasing the amount of combinations by three or more increases the web application test time.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Test all combinations of parameters (slowest):</td>
<td></td>
<td>This method of testing checks all possible combinations of attack strings with valid input to variables. Where all-pairs testing seeks to create a smaller data set as a tradeoff for speed, all combinations makes no compromise on time and uses a complete data set of tests. This testing method may take a long time to complete.</td>
</tr>
<tr>
<td>Do not stop after first flaw is found per web page</td>
<td>Cleared</td>
<td>This setting determines when a new flaw is targeted. This applies at the script level. Finding an XSS flaw does not disable searching for SQL injection or header injection, but unless otherwise specified, there is at most one report for each type on a given port. Note that several flaws of the same type (e.g., XSS, SQLi, etc.) may be reported if the flaws were caught by the same attack. This setting has three options:</td>
</tr>
<tr>
<td>Stop after one flaw is found per web server (fastest):</td>
<td></td>
<td>As soon as a flaw is found on a web server by a script, Tenable.io Web Application Scanning stops and switches to another web server on a different port.</td>
</tr>
<tr>
<td>Stop after one flaw is found per para-</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Setting

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>meter (slow):</strong> As soon as one type of flaw is found in a parameter of a CGI (e.g., XSS), Tenable.io Web Application Scanning switches to the next parameter of the same CGI, the next known CGI, or to the next port or server.</td>
<td><strong>Look for all flaws (slowest):</strong> Perform extensive tests regardless of flaws found. This option can produce a very verbose report and is not recommend in most cases.</td>
<td></td>
</tr>
<tr>
<td><strong>URL for Remote File Inclusion</strong></td>
<td><a href="http://rfi.nessus.org/rfi.txt">http://rfi.nessus.org/rfi.txt</a></td>
<td>During Remote File Inclusion (RFI) testing, this setting specifies a file on a remote host to use for tests. By default, Tenable.io Web Application Scanning uses a safe file hosted by Tenable for RFI testing. If the scanner cannot reach the Internet, you can use an internally hosted file for more accurate RFI testing.</td>
</tr>
<tr>
<td><strong>Maximum run time (minutes)</strong></td>
<td>5</td>
<td>This option manages the amount of time, in minutes, spent performing web application tests. This option defaults to 60 minutes and applies to all ports and CGIs for a given website. Scanning the local network for web sites with small applications typically completes in under an hour, however web sites with large applications may require a higher value.</td>
</tr>
</tbody>
</table>

### Report Settings
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Override normal verbosity</td>
<td>Cleared</td>
<td>This setting has two options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>I have limited disk space. Report as little information as possible:</strong> Provides less information about plugin activity in the report to minimize impact on disk space.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Report as much information as possible:</strong> Provides more information about plugin activity in the report.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Show missing patches that have been superseded</td>
<td>Selected</td>
<td>If enabled, includes superseded patch information in the scan report.</td>
</tr>
<tr>
<td>Hide results from plugins initiated as a dependency</td>
<td>Selected</td>
<td>If enabled, the list of dependencies is not included in the report. If you want to include the list of dependencies in the report, disable this setting.</td>
</tr>
<tr>
<td>Output</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow users to edit scan results</td>
<td>Selected</td>
<td>When enabled, allows users to delete items from the report. When performing a scan for regulatory compliance or other types of audits, disable the setting to show that the scan was not tampered with.</td>
</tr>
<tr>
<td>Designate hosts by their DNS name</td>
<td>Cleared</td>
<td>Uses the host name rather than IP address for report output.</td>
</tr>
<tr>
<td>Display hosts that respond to</td>
<td>Cleared</td>
<td>Reports hosts that successfully respond to a ping.</td>
</tr>
</tbody>
</table>
### Advanced Settings

The **Advanced** settings provide increased control over scan efficiency and the operations of a scan, as well as the ability to enable plugin debugging.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable safe checks</td>
<td>Selected</td>
<td>When enabled, this setting disables all plugins that may have an adverse effect on the remote host.</td>
</tr>
<tr>
<td>Stop scanning hosts that become unresponsive during the scan</td>
<td>Cleared</td>
<td>When enabled, Tenable.io Web Application Scanning stops scanning if it detects that the host has become unresponsive. This may occur if users turn off their PCs during a scan, a host stops responding after a denial of service plugin, or a security mechanism (for example, an IDS) starts to block traffic to a server. Normally, continuing scans on these machines sends unnecessary traffic across the network and delays the scan.</td>
</tr>
<tr>
<td>Scan IP addresses in a random order</td>
<td>Cleared</td>
<td>By default, Tenable.io Web Application Scanning scans a list of IP addresses in sequential order. When enabled, Tenable.io Web Application Scanning scans the list of hosts in a random order across the entire target IP space. This is typically useful in helping to distribute the network traffic during large scans.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Create unique identifier on hosts scanned using credentials</td>
<td>Selected</td>
<td>When selected, Tenable.io Web Application Scanning creates a unique identifier for credentialed scans.</td>
</tr>
<tr>
<td><strong>Performance Options</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slow down the scan when network congestion is detected</td>
<td>Cleared</td>
<td>This enables Tenable.io Web Application Scanning to detect when it is sending too many packets and the network pipe is approaching capacity. If detected, Tenable.io Web Application Scanning throttles the scan to accommodate and alleviate the congestion. Once the congestion has subsided, Tenable.io Web Application Scanning automatically attempts to use the available space within the network pipe again.</td>
</tr>
<tr>
<td>Use Linux kernel congestion detection</td>
<td>Cleared</td>
<td>This enables Tenable.io Web Application Scanning to use the Linux kernel to detect when it is sending too many packets and the network pipe is approaching capacity. If detected, Tenable.io Web Application Scanning throttles the scan to accommodate and alleviate the congestion. Once the congestion has subsided, Tenable.io Web Application Scanning automatically attempts to use the available space within the network pipe again.</td>
</tr>
<tr>
<td>Network timeout (in seconds)</td>
<td>5</td>
<td>The time that Tenable.io Web Application Scanning waits for a response from a host unless otherwise specified within a plugin. If you plan to scan over a slow connection, you may wish to set this to a greater number of seconds.</td>
</tr>
<tr>
<td>Max simultaneous checks per host</td>
<td>5</td>
<td>The maximum number of checks a Tenable.io Web Application Scanning scanner performs against a single host at one time.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Max simultaneous hosts per scan</td>
<td>30</td>
<td>The maximum number of hosts that a Tenable.io Web Application Scanning scanner scans simultaneously.</td>
</tr>
<tr>
<td>Max number of concurrent TCP sessions per host</td>
<td>None</td>
<td>The maximum number of established TCP sessions for a single host. This TCP throttling option also controls the number of packets per second the SYN scanner eventually sends (e.g., if this option is set to 15, the SYN scanner sends up to 1500 packets per second).</td>
</tr>
<tr>
<td>Max number of concurrent TCP sessions per scan</td>
<td>None</td>
<td>This setting limits the maximum number of established TCP sessions for the entire scan, regardless of the number of host scanned. For scanners installed on any Windows host, this value must be set to 19 or less to get accurate results.</td>
</tr>
</tbody>
</table>

**Debug Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable plugin debugging</td>
<td>Disabled</td>
<td>This attaches available debug logs from plugins to the vulnerability output of this scan.</td>
</tr>
</tbody>
</table>

**Credentials**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication method</td>
<td>HTTP login form</td>
<td>There are four types of HTTP Authentication methods:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Automatic authentication</strong>: Requires a username and password only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Basic/Digest authentication</strong>: Requires a user-name and password only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>HTTP login form</strong>: Requires a user to specify set-</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Settings to control where authenticated testing of a custom web-based application begins.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>HTTP cookies import</strong>: Requires a user to upload an HTTP cookie file.</td>
</tr>
<tr>
<td>Username</td>
<td>None</td>
<td>Username of the specified user.</td>
</tr>
<tr>
<td>Password</td>
<td>None</td>
<td>Password of the specified user.</td>
</tr>
<tr>
<td>Login page</td>
<td>None</td>
<td>The absolute path to the login page of the application, e.g., /login.html.</td>
</tr>
<tr>
<td>Login submission page</td>
<td>None</td>
<td>The action parameter for the form method. For example, the login form for <code>&lt;form method=&quot;POST&quot; name=&quot;auth_form&quot; action=&quot;/login.php&quot;&gt;</code> would be /login.php.</td>
</tr>
<tr>
<td>Login parameters</td>
<td>None</td>
<td>The authentication parameters (e.g., login-n=%USER%&amp;password=%PASS%). If the keywords %USER% and %PASS% are used, the keywords will be substituted with values supplied on the Login configurations drop-down menu. This field can be used to provide more than two parameters if required (e.g., a group name or some other piece of information is required for the authentication process).</td>
</tr>
<tr>
<td>Check authentication on page</td>
<td>None</td>
<td>The absolute path of a protected web page that requires authentication, to better assist Tenable.io Web Application Scanning in determining authentication status (e.g., /admin.html).</td>
</tr>
<tr>
<td>Pattern to verify successful authentication</td>
<td>None</td>
<td>A regex pattern to look for on the login page. Simply receiving a 200 response code is not always sufficient to determine session state. Tenable.io Web Application Scanning can attempt to match a given string</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cookies file</td>
<td>None</td>
<td>This option appears only if you select <strong>HTTP cookies import</strong> in the <strong>Authentication method</strong> box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To facilitate web application testing, Tenable.io Web Application Scanning can import HTTP cookies from another piece of software (e.g., web browser, web proxy, etc.) with the HTTP cookies import settings. A cookie file can be uploaded so that Tenable.io Web Application Scanning uses the cookies when attempting to access a web application. The cookie file must be in Netscape format.</td>
</tr>
</tbody>
</table>

**Global Credential Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login method</td>
<td>POST</td>
<td>The login action is performed via either a GET or POST request.</td>
</tr>
<tr>
<td>Re-authenticate delay (seconds)</td>
<td>0</td>
<td>The time delay between authentication attempts. This is useful to avoid triggering brute force lockout mechanisms.</td>
</tr>
<tr>
<td>Follow 30x redirects (number of levels)</td>
<td>0</td>
<td>If a 30x redirect code is received from a web server, this option directs Tenable.io Web Application Scanning to follow the redirect.</td>
</tr>
<tr>
<td>Invert authenticated regex</td>
<td>Cleared</td>
<td>A regex pattern to look for on the login page, that if found, tells Tenable.io Web Application Scanning authentication was not successful (e.g., Authentication failed!).</td>
</tr>
<tr>
<td>Use authenticated regex on HTTP headers</td>
<td>Cleared</td>
<td>Tenable.io Web Application Scanning can search the HTTP response headers (rather than the body) for a given regex pattern to better determine authentication state.</td>
</tr>
</tbody>
</table>
### PCI WAS Scan

**Note:** You can use only the classic interface to [create](#) or [modify](#) a scan or user-defined template based on the **PCI WAS Scan** template. For more information, see [Interface Activation Modes in WAS](#).

## Basic Settings

### General

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>None</td>
<td>The name of the scan or policy. This value appears in the Tenable.io interface.</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>None</td>
<td>A description of the scan or policy.</td>
<td>No</td>
</tr>
<tr>
<td>Folder</td>
<td>My Scans</td>
<td>The folder where the scan appears after saving.</td>
<td>Yes</td>
</tr>
<tr>
<td>Scanner</td>
<td>Varies</td>
<td>The scanner that performs the scan. The default scanner varies based on the organization and user.</td>
<td>Yes</td>
</tr>
<tr>
<td>Target</td>
<td>None</td>
<td>The target you want to scan, in URL format. The URL for the target you want to scan, as is appears on your Tenable.io Web Application Scanning license.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Note:** If the URL you type in the **Target** box has a different FQDN host from the URL that appears on your license, and your scan runs...
### Setting

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>successfully, the new URL you type counts as an additional asset on your license.</td>
</tr>
</tbody>
</table>

### Schedule

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Off</td>
<td>The toggle that specifies whether the scan is scheduled. By default, scans are not scheduled. To modify the following <strong>Schedule</strong> settings, click the <strong>Off</strong> button.</td>
</tr>
<tr>
<td>Frequency</td>
<td>Once</td>
<td>How often the scan launches.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The frequency with which you scan your target depends on several factors (e.g., how often you update your web application, the content your web application contains, etc.). For most web applications, Tenable recommends at least monthly scans.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Once:</strong> Schedule the scan at a specific time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Daily:</strong> Schedule the scan to occur on a daily basis, at a specific time, for up to 20 days.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Weekly:</strong> Schedule the scan to occur on a recurring basis, by time and day of week, for up to 20 weeks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Monthly:</strong> Schedule the scan to occur every month, by time and day of month or week of month, for up to 20 months.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Yearly:</strong> Schedule the scan to occur every year, by time and day, for up to 20 years.</td>
</tr>
<tr>
<td>Starts</td>
<td>Varies</td>
<td>The exact date and time when a scan launches.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> If you schedule an excessive number of scans to run concurrently, you may exhaust the scanning capacity on Tenable.io</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Web Application Scanning</td>
<td></td>
<td>Web Application Scanning. If necessary, Tenable.io Web Application Scanning staggers concurrent scans to ensure consistent scanning performance.</td>
</tr>
<tr>
<td>Timezone</td>
<td>Zulu</td>
<td>The timezone of the value set for Starts.</td>
</tr>
<tr>
<td>Summary</td>
<td>Not applicable</td>
<td>A summary of the schedule for your scan based on the values you have specified for the available settings.</td>
</tr>
</tbody>
</table>

### Notifications

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Recipient(s)</td>
<td>None</td>
<td>The email addresses that are alerted when a scan completes and the results are available.</td>
</tr>
</tbody>
</table>

### Permissions

Using settings in the Permissions section, you can assign various permissions to groups and individual users. When you assign a permission to a group, that permission applies to all users within the group. The following rows describe the permissions that can be assigned.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add users or groups</td>
<td>The users or groups to which you want to apply permissions.</td>
</tr>
<tr>
<td>No access</td>
<td>Groups and users set to <strong>No access</strong> cannot interact with the scan in any way.</td>
</tr>
</tbody>
</table>

**Note:** When you apply a permission to a group, the permission applies to all users within the group. The following rows describe the permissions that you can assign.
When you create a scan or policy, no other users or groups have access to it by default.

- **Can view**: Groups and users set to **Can view** can view the results of the scan.
- **Can control**: Groups and users set to **Can control** can launch, pause, and stop a scan, as well as view its results.
- **Can configure**: Groups and users set to **Can configure** can modify the configuration of the scan in addition to all other permissions.

### Scope Settings

The **Scope** settings specify URLs and file types that you want to include or exclude from your scan.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Inclusion</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List of URLs</td>
<td>None</td>
<td>A text box in which you can type URLs to include in the scan.</td>
</tr>
<tr>
<td>Specify how the scanner handles URL's found during the application crawl</td>
<td>Cleared</td>
<td>This setting has three options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Crawl all URLs detected</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Limit crawling to specified URLs and child paths</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Limit crawling to specified URLs</strong></td>
</tr>
</tbody>
</table>

**Note**: To increase your scan's coverage and effectiveness, Tenable recommends that you first run an **Overview** scan and review the output for the [Web Application Sitemap plugin](#). Then, determine how to modify your configurations to refine the scope and eliminate redundant web pages.
### Setting

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regex for excluded URLs</td>
<td>logout</td>
<td>A text box in which you can specify in-scope URL regex values to exclude from the scan. For example, if you type &quot;logout&quot;, then any in-scope URL that includes the word &quot;logout&quot; is excluded.</td>
</tr>
<tr>
<td>File extensions to exclude</td>
<td>css, js, png, jpeg, gif, pdf, csv</td>
<td>A text box in which you can type file types to exclude from the scan.</td>
</tr>
</tbody>
</table>

### Discovery Settings

The **Discovery** settings include configurable settings that allow the scan to discover new URLs other than the ones discovered during crawling.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL Parameter Manipulation</td>
<td>Cleared</td>
<td>Whether the scanner will change values found in a query string, and resubmits the URL to discover new pages.</td>
</tr>
<tr>
<td>Maximum Manipulation Attempts</td>
<td>10</td>
<td>The maximum number of times the scanner will attempt to manipulate query string values.</td>
</tr>
<tr>
<td>Crawl Scripts</td>
<td>None</td>
<td>A link to upload one or more Selenium scripts to crawl during the scan. For more information, see the Selenium instructions in <a href="http://example.com">Web App Authentication</a>.</td>
</tr>
</tbody>
</table>

### Assessment Settings

The **Assessment** settings include configurable settings that allow the scan to audit elements other than the ones discovered during crawling. If you select **Custom** in the **Scan Type** drop-down box, the **General** section appears.
**Note:** When you select a check box for an option in the **Elements** section, the scanner analyzes that element type and tests all instances of the element for security vulnerabilities (e.g., OWASP Top 10).

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Elements</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit cookies</td>
<td>Selected</td>
<td>The scan checks for cookie-based vulnerabilities.</td>
</tr>
<tr>
<td>Audit forms</td>
<td>Selected</td>
<td>The scan checks for form-based vulnerabilities.</td>
</tr>
<tr>
<td>Audit headers</td>
<td>Selected</td>
<td>The scan inspects headers for vulnerabilities and insecure configurations (e.g., missing X-Frame-Options).</td>
</tr>
<tr>
<td>Audit links</td>
<td>Selected</td>
<td>The scan includes links and their parameters in vulnerability checks.</td>
</tr>
<tr>
<td>Audit parameter names</td>
<td>Cleared</td>
<td>The scan performs extensive fuzzing of parameter names.</td>
</tr>
<tr>
<td>Audit parameter values</td>
<td>Selected</td>
<td>The scan performs extensive fuzzing of parameter values.</td>
</tr>
<tr>
<td>Audit JSON</td>
<td>Cleared</td>
<td>The scan audits JSON request data.</td>
</tr>
<tr>
<td>Audit XML</td>
<td>Cleared</td>
<td>The scan audits XML request data.</td>
</tr>
<tr>
<td>Audit UI Forms</td>
<td>Selected</td>
<td>The scan checks input and button groups associated with JavaScript code.</td>
</tr>
<tr>
<td>Audit UI Inputs</td>
<td>Selected</td>
<td>The scan checks orphan input elements with associated DOM events.</td>
</tr>
<tr>
<td><strong>Options</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL for Remote File</td>
<td><a href="http://rfi.nessus.org/RFI.txt">http://rfi.nessus.org/RFI.txt</a></td>
<td>During Remote File Inclusion (RFI) testing, this setting specifies a file on a remote host to</td>
</tr>
</tbody>
</table>
### Setting | Default Value | Description
--- | --- | ---
Inclusion |  | use for tests. By default, Tenable.io uses a safe file hosted by Tenable for RFI testing. If the scanner cannot reach the Internet, you can use an internally hosted file for more accurate RFI testing.

### Advanced Settings
The **Advanced** settings provide increased control over scan efficiency and the operations of a scan, as well as the ability to enable plugin debugging.

### General

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overall Scan max time (HH:MM:SS)</td>
<td>08:00:00</td>
<td>The maximum duration the scan runs before it stops automatically. <strong>Note:</strong> The maximum duration you can set for your overall scan max time is 99:59:59 (hours: minutes: seconds).</td>
</tr>
<tr>
<td>Enable Debug logging for this scan</td>
<td>Off</td>
<td>A check box that, when selected, adds additional information to the scan's log to assist with debugging. <strong>Note:</strong> Tenable recommends that you leave this setting off unless Tenable Support instructs you to enable it.</td>
</tr>
<tr>
<td><strong>Limits</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of URLs to Crawl and Browse</td>
<td>10000</td>
<td>The maximum number of URLs the scanner attempts to crawl and, therefore, audit.</td>
</tr>
<tr>
<td>Path Directory</td>
<td>10</td>
<td>The maximum number of sub-directories the scanner</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Depth</td>
<td></td>
<td>crawls.</td>
</tr>
<tr>
<td>Page DOM Element Depth</td>
<td>5</td>
<td>The maximum depth of HTML nested elements the scanner crawls.</td>
</tr>
<tr>
<td>Maximum Response Size</td>
<td>500000</td>
<td>The maximum load size of a page in order to be audited. If the scanner crawls a URL and the response exceeds the limit, then it is not audited and no vulnerability assessment is performed.</td>
</tr>
<tr>
<td>Request Redirect Limit</td>
<td>1</td>
<td>The number of redirects the scan follows before it stops trying to crawl the page.</td>
</tr>
</tbody>
</table>

### Discovery

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Crawl Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Agent</td>
<td>WAS/%v</td>
<td>The user-agent header used by the scanner when sending an HTTP request.</td>
</tr>
<tr>
<td>Note: The %v placeholder indicates the version of the scan engine.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom Headers</td>
<td>None</td>
<td>A list of custom headers you want to inject into each HTTP request.</td>
</tr>
<tr>
<td>Note: If you specify the user-agent value in this list, that value will override the value entered in the User Agent box.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Screen Settings - settings of the virtual browser instance spun up by the scanner</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Screen Width</td>
<td>1600</td>
<td>The screen width, in pixels, of the browser embedded into the scanner.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Screen Height</td>
<td>1200</td>
<td>The screen height, in pixels, of the browser embedded into the scanner.</td>
</tr>
<tr>
<td>Ignore Images</td>
<td>Selected</td>
<td>Whether images on web pages should be crawled or ignored by the browser embedded into the scanner.</td>
</tr>
</tbody>
</table>

**Selenium Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page rendering delay</td>
<td>10000</td>
<td>The time, in milliseconds, to allow the browser to render the page.</td>
</tr>
<tr>
<td>Command execution delay</td>
<td>500</td>
<td>The time, in milliseconds, to wait after processing a command before processing a new one.</td>
</tr>
<tr>
<td>Script completion delay</td>
<td>5000</td>
<td>The time, in milliseconds, to wait once all commands are processed for rendering new content.</td>
</tr>
</tbody>
</table>

**Performance**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max number of concurrent HTTP connections</td>
<td>10</td>
<td>The maximum number of established HTTP sessions for a single host.</td>
</tr>
<tr>
<td>Max number of HTTP requests per second</td>
<td>25</td>
<td>The maximum number of HTTP requests for the entire scan for a single host.</td>
</tr>
<tr>
<td>Slow down the scan when network congestion is detected</td>
<td>Selected</td>
<td>Whether the scan is throttled when it detects network congestion.</td>
</tr>
<tr>
<td>Network timeout (in seconds)</td>
<td>5</td>
<td>The time that the scanner waits for a response from a host, unless otherwise specified within a plugin.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Browser timeout (in seconds)</td>
<td>10</td>
<td>The time that the scanner waits for a response from a browser, unless otherwise specified within a plugin. If you are scanning over a slow connection, you may wish to set this to a higher number of seconds.</td>
</tr>
<tr>
<td>Timeout threshold</td>
<td>100</td>
<td>The number of consecutive timeouts before the scan aborts (minimum 100).</td>
</tr>
</tbody>
</table>

### Plugins

You can enable or disable individual plugins and/or plugin families to customize your scan. When you click on a plugin, the following details appear:

- **Description**: A description of the discovered vulnerability.
- **Solution**: The steps that you can take to mitigate the discovered vulnerability.
- **Plugin Information**: The Plugin ID, publication date, and last modified date.
- **Risk Information**: The risk factor of the discovered vulnerability.

### Credentials

The **Web App Scan** scan template offers three different authentication methods:

- **HTTP Server Authentication**: authenticates toward the server.
- **Web Application Authentication - Login Form**: authenticates toward the application.
- **Web Application Authentication - Cookie Authentication**: authenticates toward the session.

**Note**: If the scan fails to authenticate, it aborts immediately with a message explaining that it could not authenticate.
## HTTP Server Authentication

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>None</td>
<td>The user name of the authorized user. For example, the user name of one of the users listed in the <code>htpasswd</code> file on an Apache server.</td>
</tr>
<tr>
<td>Password</td>
<td>None</td>
<td>The password of the authorized user.</td>
</tr>
</tbody>
</table>

## Web Application Authentication

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Method</td>
<td>Login Form</td>
<td>Allows you specify whether you want to use a login form or cookie authentication to authenticate the scan.</td>
</tr>
</tbody>
</table>

Depending on which option you select, the following options will appear:

### Login Form

- Login Page
- Credentials
- Pattern to verify successful auth
- Page to verify active session
- Pattern to verify active session

### Cookie Authentication

- Session Cookies
- Page to verify active session
- Pattern to verify active session
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Page</td>
<td>None</td>
<td>The URL that is specified in the form action attribute and used to submit the form authentication. This may not be the URL for the login form.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> This parameter accepts relative or absolute URLs.</td>
</tr>
<tr>
<td>Credentials</td>
<td>None</td>
<td>One or more key value pairs to perform authentication. The pairs are concatenated upon submission to create the list of parameters required by the form. For instructions on how to retrieve the key value pairs, see Configure WAS Login Form Authentication (Classic Interface).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The form may require more than just the user name and password parameters, so you must provide all parameters required by the form to ensure proper authentication.</td>
</tr>
<tr>
<td>Pattern to verify successful auth</td>
<td>None</td>
<td>The regular expression to be matched against the form submission response to verify that the login was successful.</td>
</tr>
<tr>
<td>Session Cookies</td>
<td>None</td>
<td>One or more key value pairs to perform authentication. The pairs are concatenated upon submission to create the list of parameters required by the form. For instructions on how to retrieve the key value pairs, see WAS Cookie Authentication (Classic Interface).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The form may require more than just the user name and password parameters, so you must provide all parameters required by the form to ensure proper authentication.</td>
</tr>
</tbody>
</table>

**Global Credential Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page to verify active session</td>
<td>None</td>
<td>The URL used to verify if the scan is authenticated.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Pattern to verify active session</td>
<td>None</td>
<td>The regular expression to be matched against the contents of the URL specified by the <strong>Page to verify active session</strong> parameter to verify if the scan is authenticated.</td>
</tr>
</tbody>
</table>
Agent Templates (Classic Interface)

You can use templates to create an agent scan or policy.

In both Nessus Manager and Tenable.io, default templates for agent scans appear in the Agent tab. The manager interface provides brief explanations of each default template.

**Note:** If you create custom policies for agent scans, those templates appear in the User Defined tab.

The table below briefly describes the settings for the default agent scan templates. You may also have access to special templates.

For a comprehensive explanation of template settings, see the documentation for Nessus Manager or Tenable.io.

### Agent Templates

Agent templates fall into two categories: **Vulnerabilities** and **Compliance**.

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerabilities</strong></td>
<td></td>
</tr>
<tr>
<td>Advanced Agent Scan</td>
<td>Scans without any recommendations.</td>
</tr>
<tr>
<td><strong>Note:</strong> When you create an agent scan using the Advanced Agent Scan template, you must also select the plugins you want to use for the scan.</td>
<td></td>
</tr>
<tr>
<td>Basic Agent Scan</td>
<td>Scans systems connected via Nessus Agents.</td>
</tr>
<tr>
<td>Malware Scan</td>
<td>Scans for malware on systems connected via Nessus Agents.</td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
<td></td>
</tr>
<tr>
<td>Policy Compliance Auditing</td>
<td>Audits systems connected via Nessus Agents.</td>
</tr>
<tr>
<td>Template</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>SCAP and OVAL Auditing</td>
<td>Audits systems using SCAP and OVAL definitions.</td>
</tr>
</tbody>
</table>
Scan and Policy Settings (Classic Interface)

Scan settings enable you to refine parameters in scans to meet your specific network security needs. The scan settings you can configure vary depending on the Tenable-provided template on which a scan or policy is based.

You can configure these settings in individual scans or in policy from which you create individual scans. For example:

**Note:** The following image is an example of the way settings are organized in the Tenable.io interface.

The documentation is organized to reflect the interface. For example, this topic contains information about the Settings tab in a scan or policy (1 in the image). You can also find information about the Basic settings as a category (2 in the image), which includes settings in the General section specifically (3 in the image).

Scan settings are organized into the following categories:

- Basic Settings for Scans
- Basic Settings for Policies
- Discovery Settings
- Assessment Settings
- Report Settings
- Advanced Settings
- Credentials (Classic Interface)
Settings in Policies

When configuring settings for policies, note the following:

- If you configure a setting in a policy, that setting applies to any scans you create based on that policy.

- You base a policy on a Tenable-provided template. Most of the settings are identical to the settings you can configure in an individual scan that uses the same Tenable-provided template. However, certain Basic settings are unique to creating a policy, and do not appear when configuring an individual scan. For more information, see Basic Settings for Policies (Classic Interface).

- You can configure certain settings in a policy, but cannot modify those settings in an individual scan based on a policy. These settings include Discovery, Assessment, Report, Advanced, Compliance, SCAP, and Plugins. If you want to modify these settings for individual scans, create individual scans based on a Tenable-provided template instead.

- If you configure Credentials in a policy, other users can override these settings by adding scan-specific or managed credentials to scans based on the policy.
Configure Scan Settings (Classic Interface)

<table>
<thead>
<tr>
<th>Required Tenable.io Vulnerability Management User Role:</th>
<th>Scan Operator, Standard, Scan Manager, or Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required Tenable.io Web Application Scanning User Role:</td>
<td>Scan Operator, Standard, Scan Manager, or Administrator</td>
</tr>
<tr>
<td>Required Scan Permissions:</td>
<td>Can Configure</td>
</tr>
</tbody>
</table>

To configure scan settings:

1. In the top navigation bar, click **Scans**.
   
The **My Scans** page appears.

2. (Optional) In the left navigation bar, click a different folder.

3. In the scans table, select the check box next to the scan you want to configure.
   
   In the upper-right corner, the **More** button appears.

4. Click the **More** button.

5. Click **Configure**.
   
The **Configuration** page for that scan appears.

6. Modify the **settings**.

7. Click the **Save** button.

---

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
WAS Credentials (Classic Interface)

**Note:** The topics in this section describe credentials in the classic interface only. If you activate the new interface, you can view a snapshot of historical credentials that you configured in the classic interface, but you cannot modify those credentials.

For information about credentials in the new interface, see [Credentials in WAS Scans](#).

Tenable.io Web Application Scanning supports the following forms of authentication:

- [Server Based Authentication](#)
- [Web App Authentication](#)
- [Cookie Authentication](#)
WAS Server-Based Authentication (Classic Interface)

**Required Additional License:** Tenable.io Web Application Scanning

**NTLM**

To use NTLM authentication:

1. Click **Scans > New Scan > Web Application**

2. Click the tile for the scan template type you want to authenticate.

   **Note:** NTML authentication is not supported in the **Legacy Web App Scan** template.

   The new scan template page appears.

3. Click the **Credentials** tab.

   The **Add Managed Credentials** page appears.

4. In the **Add Credentials** section, click **HTTP Server Authentication**.

5. In the **Username** text box, type your username.

6. In the **Password** text box, type your password.

7. From the **Authentication Type** drop-down box, select **NTLM**.

8. Click **Save to Managed Credentials**.

**Basic / Digest**

To use Basic / Digest Authentication:

1. Click **Scans > New Scan > Web Application**

2. Click the tile for the scan template type you want to authenticate.

   The new scan template page appears.

3. Click the **Credentials** tab.
The **Add Managed Credentials** page appears.

4. In the **Add Credentials** section, click **HTTP Server Authentication**.

5. In the **Username** text box, type your username.

6. In the **Password** text box, type your password.

7. From the **Authentication Type** drop-down box, select **NTLM**.

8. Click **Save to Managed Credentials**.
Configure WAS Login Form Authentication (Classic Interface)

**Required Additional License:** Tenable.io Web Application Scanning

These steps describe how to check the authentication values for the Login Form authentication option in the **Credentials** settings for the Web App Overview and Web App Scan templates.

These steps assume that you already have a login form ready to test your credentials.

To test your authentication values in the classic interface:

1. For the web application you want to scan, access the login page.
2. Type your credentials.
3. Upon successful authentication, in the browser console, locate the call that performs the authentication. In this example, the call is `login`.

   The **Form Data** section of the **Headers** tab displays the key/value pairs. In this example, the
pairs are uname: Nessus, upass: WAS, and udomain: Tenable.io.

To run a credentialed scan with login form authentication:

1. In Tenable.io Web Application Scanning, either create a new scan, or access the scan settings for which you want to add credentials.
2. In the scan settings, click the Credentials tab.
3. Click Web Application Authentication.
   a. In the Authentication Method drop-down box, select Login Form.
   b. In the Login Page box, type the URL for your login form page.
   c. In the Credentials boxes, type the key/value pairs that you retrieved in step 3 of To test your authentication values.
   d. In the Pattern to verify successful auth box, type the regex to match when the credentials are correct.

   **Note:** In many cases, the regex is text that appears on the login page (e.g., Welcome!)

   e. In the Page to verify active session box, type the URL you want to use to verify if the session is still active.
   f. In the Pattern to verify active session box, type the regex to match to confirm the session is still active.
4. Click the Save button.
WAS Cookie Authentication (Classic Interface)

Required Additional License: Tenable.io Web Application Scanning

These steps describe how to check the authentication values for the Cookie Authentication option in the Credentials settings for the Web App Overview and Web App Scan templates in the classic interface.

These steps assume that you already have a cookie authentication form ready to test your credentials.

To test your authentication values:

1. For the web application you want to scan, access the cookie authentication page.
2. Type your credentials.

3. Upon successful authentication, in the browser console, locate the call that performs the authentication. In this example, the call is login.

   The Cookies tab displays one or more key/value pairs. In this example, the pair is was-
session and Tenable.io.

To run a credentialed scan with cookie authentication:

1. In Tenable.io Web Application Scanning, either create a new scan, or go to the scan settings for which you want to add credentials.
2. In the scan settings, click the Credentials tab.
3. Click Web Application Authentication.
4. In the Authentication Method drop-down box, select Cookie Authentication.
5. In the Session Cookies text box, type the key/value pairs that you retrieved in step 3 of To test your authentication values.
6. In the Page to verify active session text box, type the URL you want to use to verify if the session is still active.
7. In the Pattern to verify active session text box, type the regex to match to confirm the session is still active.

**Note:** In many cases, the regex is text that appears on the login page (e.g., Welcome!)

8. Click Save.

When you launch the scan, the Cookie Authentication Succeeded plugin appears in the scan results.
If the **Cookie Authentication Failed** plugin appears, the output indicates the reason for the failure.

If the page did not authenticate successfully, there is an issue with the cookies sent to the scan.

If the page did authenticate successfully, there may be an issue with the regex you defined.
**INFO**  Cookie Authentication Failed

**Description**
This plugin is raised when the scanner has not been able to authenticate against the web application using the cookies provided in the scan policy. Check the output of the plugin to get an explanation of the issue encountered by the scan.

**Solution**
Edit scan policy and update the cookies using the information provided in the plugin output.

**URLs**
- https://session

**Output**
Authentication check on URL 'https://session' failed. When requesting 'https://session' the response did not contain the pattern 'Welcome John' which was expected if the session was authenticated.

The following cookies were used in the request:
- Tenable.io-

Check the response provided as an attachment and verify what text can be used to check if the session is authenticated.

**Attachments**
- Check Auth URI Request Headers
- Check Auth URI Response Headers
- Check Auth URI Response
Configure WAS Selenium Authentication (Classic Interface)

**Required Additional License:** Tenable.io Web Application Scanning

These steps describe how to create a Selenium script to use with the Selenium Authentication option in the Credentials settings for the Web App Overview and Web App Scan templates.

These steps assume that you are using Google Chrome as your browser and have downloaded the Selenium IDE extension from the Chrome Web Store.

To create a script to log in with your credentials:

1. For the web application you want to scan, access the login page in Google Chrome.

   ![Login Form Testing page](image)

   This login form requires 3 params to be set: user, pass, domain
   Successful login: Nessus, WAS, Tenable.io

2. In the upper right corner of the browser window, click the button to launch the Selenium IDE extension.

   The Selenium IDE window appears.
3. In the upper right corner of the Selenium IDE window, click the √ button to begin the recording.

4. On the login page, enter your credentials and submit. Selenium IDE captures your actions.

5. In the upper right corner of the Selenium IDE window, click the □ button to stop the recording.

6. Click the  button to save the project.

To run a credentialed scan with Selenium authentication:

1. In Tenable.io Web Application Scanning, either create a new scan, or access the scan settings for which you want to add credentials.
2. In the scan settings, click the **Credentials** tab.

3. Click **Web Application Authentication**.
   
a. In the **Authentication Method** drop-down box, select **Selenium Authentication**.
   
b. Click **Add File**, and select the `.side` project that you saved in step 6 of **To create a script to log in with your credentials**.
   
c. In the **Page to verify active session** box, type the URL you want to use to verify if the session is still active.
   
d. In the **Pattern to verify active session** box, type the regex to match to confirm the session is still active.

   **Note:** In many cases, the regex is text that appears on the login page (e.g., `Welcome!`)

4. Click the **Save** button.

   When you launch the scan, the Selenium script will run and authenticate for you.
Set Scan Permissions (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can Configure

To set scan permissions:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. (Optional) In the left navigation bar, click a different folder.

3. In the scans table, select the check box next to the scan you want to configure.
   
   In the upper-right corner, the **More** button appears.

4. Click **More**.

5. In the **Settings** tab, under **Basic**, click **Permissions**.
   
   The permissions settings appear.

6. Modify the permissions settings.

7. Click the **Save** button.
   
   Tenable.io updates the scan permissions.
Basic Settings for Scans (Classic Interface)

Note: This topic describes Basic settings you can set in scans. For Basic settings in policies, see Basic Settings for Policies.

The Basic scan settings are used to specify certain organizational and security-related aspects of the scan, including the name of the scan, its targets, whether the scan is scheduled, and who has access to the scan, among other settings.

Configuration items that are required by a particular scan are indicated in the Tenable.io interface.

The Basic settings include the following sections:

- General
- Targets
- Schedule
- Notifications
- Permissions

The following tables list all available Basic settings by section.

General

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>None</td>
<td>Specifies the name of the scan.</td>
</tr>
<tr>
<td>Description</td>
<td>None</td>
<td>(Optional) Specifies a description of the scan.</td>
</tr>
<tr>
<td>Scan Results</td>
<td>Show in dashboard</td>
<td>Specifies whether the results of the scan should appear in dashboards or be kept private.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When set to Keep private, you must access the scan directly to view the results.</td>
</tr>
<tr>
<td>Folder</td>
<td>My Scans</td>
<td>Specifies the folder where the scan appears after being saved.</td>
</tr>
<tr>
<td><strong>Agent Groups</strong></td>
<td>None</td>
<td>(Agent scans only) Specifies the agent group or groups you want the scan to target. Select an existing agent group from the drop-down box, or create a new agent group. For more information, see <a href="#">Create a New Agent Group</a>.</td>
</tr>
<tr>
<td>------------------</td>
<td>------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Scan Window</strong></td>
<td>1 hour</td>
<td>(Agent scans only) (Required) Specifies the time frame during which agents must report in order to be included and visible in vulnerability reports. Use the drop-down box to select an interval of time, or click 📜 to type a custom scan window.</td>
</tr>
</tbody>
</table>
| **Scanner**      | Auto-Select | Specifies the scanner that performs the scan.  
The scanners you can select for this parameter depend on the scanners and scanner groups configured for your Tenable.io instance, as well as your permissions for those scanners or groups.  
Select a scanner based on the location of the targets you want to scan. For example:  
- Select a [scanner group](#) if you want to:  
  - Improve scan speed by balancing the scan load among multiple scanners.  
  - Rebuild scanners and link new scanners in the future without having to update scanner designations in scan configurations.  
- Select [Auto-Select](#) to enable [scan routing](#) for the targets. |
| **Tags**         | None | Select one or more [tags](#) to scan all assets that have any of the specified tags applied. To see a list of assets identified by the specified tags, click [View Assets](#). For more inform- |
| Target Groups | None | You can select or add a new target group to which the scan applies. Assets in the target group are used as scan targets.  

**Note:** You can select a target group in this option if you have Can Use permissions for the target group. You must also have Can Scan permissions in an access group for the target, or the scanner does not scan the target. |
| Policy | None | This setting appears only when the scan owner edits an existing scan that is based on a policy.  

**Note:** After scan creation, you cannot change the Tenable-provided template on which a scan is based.  

In the drop-down box, select a policy on which to base the scan. You can select policies for which you have Can View or higher permissions.  

In most cases, you set the policy at scan creation, then keep the same policy each time you run the scan. However, you may want to change the policy when troubleshooting or debugging a scan. For example, changing the policy makes it easy to enable or disable different plugin families, change performance settings, or apply dedicated debugging policies with more verbose logging.  

When you change the policy for a scan, the scan history retains the results of scans run under the previously-assigned policy. |
| Targets | None | Specifies one or more targets to be scanned. If you select a target group or upload a targets file, you are not required to specify additional targets.  

**Note:** Users running the scan must have Can Scan permissions in an access group for the specified target, or the scan- |
Targets

The **Targets** section appears when you have an AWS Pre-Authorized scanner configured. In the **Targets** section, you can select the AWS targets you want to scan.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan all targets</td>
<td>None</td>
<td>Select this option to scan all targets identified by AWS, including new targets identified in the future.</td>
</tr>
<tr>
<td>Scan individual targets</td>
<td>None</td>
<td>Select this option to select the individual targets you want to scan. In the target list, select the check box next to each target you want to scan and click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>
Schedule

By default, scans are not scheduled. When you first access the Schedule section, the Enable Schedule setting appears, set to Off. To modify the settings listed on the following table, click the Off button. The rest of the settings appear.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>Once</td>
<td>Specifies how often the scan is launched.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Once</strong>: Schedule the scan at a specific time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Daily</strong>: Schedule the scan to occur on a daily basis, at a specific time or to repeat up to every 20 days.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Weekly</strong>: Schedule the scan to occur on a recurring basis, by time and day of week, for up to 20 weeks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Monthly</strong>: Schedule the scan to occur every month, by time and day or week of month, for up to 20 months.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Yearly</strong>: Schedule the scan to occur every year, by time and day, for up to 20 years.</td>
</tr>
<tr>
<td>Starts</td>
<td>Varies</td>
<td>Specifies the exact date and time when a scan launches.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The starting date defaults to the date when you are creating the scan. The starting time is the nearest half-hour interval. For example, if you create your scan on 09/31/2018 at 9:12 AM, the default starting date and time is set to 09/31/2018 and 09:30.</td>
</tr>
<tr>
<td>Timezone</td>
<td>Zulu</td>
<td>Specifies the timezone of the value set for Starts.</td>
</tr>
<tr>
<td>Repeat Every</td>
<td>Varies</td>
<td>Specifies the interval at which a scan is relaunched. The</td>
</tr>
</tbody>
</table>
default value of this item varies based on the frequency you choose.

Repeat On | Varies | Specifies what day of the week a scan repeats. This item appears only if you specify Weekly for Frequency. The value for Repeat On defaults to the day of the week on which you create the scan.

Repeat By | Day of the Month | Specifies when a monthly scan is relaunched. This item appears only if you specify Monthly for Frequency.

Summary | N/A | Provides a summary of the schedule for your scan based on the values you have specified for the available settings.

Notifications

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Recipient(s)</td>
<td>None</td>
<td>Specifies zero or more email addresses, separated by commas, that are alerted when a scan completes and the results are available.</td>
</tr>
<tr>
<td>Result Filters</td>
<td>None</td>
<td>Defines the type of information to be emailed.</td>
</tr>
</tbody>
</table>

Permissions

Using settings in the Permissions section, you can assign various permissions to groups and individual users. When you assign a permission to a group, that permission applies to all users within the group. The following table describes the permissions that can be assigned.

Tip: Tenable recommends assigning permissions to user groups, rather than individual users, to minimize maintenance as individual users leave or join your organization.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Sharing</td>
<td></td>
</tr>
</tbody>
</table>
| **Scan Results** | Specifies whether the results of the scan should appear in dashboards or be kept private.  
When set to **Keep private**, you must access the scan directly to view the results. |
|-----------------|-------------------------------------------------------------------------------------------------|
| **User Sharing** | Specifies the only user who can copy the scan or change scan ownership.  
This setting is only visible if you are the scan owner. By default, you are assigned ownership when you create the scan. |
| **Owner** | Share the scan with other users by setting permissions for users or groups.  
You can set the following permissions:  
- **No Access** — (Default) Groups and users set to this permission cannot interact with the scan in any way.  
- **Can View** — Groups and users with this permission can view the results of the scan, export the scan results, and move the scan to the Trash folder. They cannot view the scan configuration or permanently delete the scan.  
- **Can Control** — In addition to the tasks allowed by **Can View**, groups and users with this permission can launch, pause, and stop a scan. They cannot view the scan configuration or permanently delete the scan.  
  
**Note:** In addition to **Can Control** permissions for the scan, users running a scan must have **Can Scan** permissions in an access group for the specified target, or the scanner does not scan the target.  
- **Can Configure** — In addition to the tasks allowed by **Can Control**, groups and users with this permission can view the scan configuration and modify any setting for the scan except scan ownership.  
  
**Note:** Only scan owners can permanently delete a scan.  
**Note:** User roles override scan permissions in the following cases:  
- A basic user cannot run a scan or configure a scan, regardless of the permissions assigned to that user in the individual scan. |
- An administrator always has the equivalent of **Can Configure** permissions, regardless of the permissions set for the administrator account in the individual scan.
Basic Settings for Policies (Classic Interface)

Note: This topic describes Basic settings you can set in policies. For Basic settings in individual scans, see Basic Settings for Scans.

You can use Basic settings to specify basic aspects of a policy, including who has access to the policy.

The Basic settings include the following sections:

- **General**
- **Permissions**
- **Authentication**

General

The general settings for a policy.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>None</td>
<td>Specifies the name of the policy.</td>
</tr>
<tr>
<td>Description</td>
<td>None</td>
<td>(Optional) Specifies a description of the policy.</td>
</tr>
</tbody>
</table>

Permissions

You can share the policy with other users by setting permissions for users or groups. When you assign a permission to a group, that permission applies to all users within the group.

Tip: Tenable recommends assigning permissions to user groups, rather than individual users, to minimize maintenance as individual users leave or join your organization.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Access</td>
<td>(Default user only) Groups and users set to this permission cannot interact with the policy in any way.</td>
</tr>
<tr>
<td>Can Use</td>
<td>Groups and users with this permission can view the policy configuration and</td>
</tr>
</tbody>
</table>
use the policy to create scans.

**Can Edit**

In addition to viewing the policy and using the policy to create scans, groups and users with this permission can modify any policy settings except user permissions and policy ownership. However, they cannot export or delete the policy.

**Can Configure**

In addition to viewing the policy and using the policy to create scans, groups and users with this permission can modify any setting for the policy except policy ownership. They can export the policy, but cannot delete the policy.

**Note:** Only the policy owner can delete a policy.

**Authentication**

In policies, you can use **Authentication** settings to configure the authentication Tenable.io performs for credentialed scanning.

**Tip:** The **Authentication** settings are equivalent to the **Scan-wide Credential Type Settings** in Tenable-provided scan templates.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv1/v2c</td>
<td></td>
<td>equivalent to Scans &gt; Credentials &gt; <strong>Plaintext Authentication</strong> &gt; SNMPv1/v2c</td>
</tr>
<tr>
<td>UDP Port</td>
<td>161</td>
<td>Ports where Tenable.io attempts to authenticate on the host device.</td>
</tr>
<tr>
<td>Additional UDP port #1</td>
<td>161</td>
<td></td>
</tr>
<tr>
<td>Additional UDP port #2</td>
<td>161</td>
<td></td>
</tr>
<tr>
<td>Additional UDP port #3</td>
<td>161</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### equivalent to Scans > Credentials > Plaintext Authentication > HTTP

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login method</td>
<td>POST</td>
<td>Specify if the login action is performed via a GET or POST request.</td>
</tr>
<tr>
<td>Re-authenticate delay (seconds)</td>
<td>0</td>
<td>The time delay between authentication attempts. Setting a time delay is useful to avoid triggering brute force lockout mechanisms.</td>
</tr>
<tr>
<td>Follow 30x redirects (# of levels)</td>
<td>0</td>
<td>If a 30x redirect code is received from a web server, this setting directs Tenable.io to follow the link provided or not.</td>
</tr>
<tr>
<td>Invert authenticated regex</td>
<td>Disabled</td>
<td>A regex pattern to look for on the login page, that if found, tells Tenable.io that authentication was not successful (e.g., Authentication failed!).</td>
</tr>
<tr>
<td>Use authenticated regex on HTTP headers</td>
<td>Disabled</td>
<td>Rather than search the body of a response, Tenable.io can search the HTTP response headers for a given regex pattern to better determine authentication state.</td>
</tr>
<tr>
<td>Case insensitive authenticated regex</td>
<td>Disabled</td>
<td>The regex searches are case sensitive by default. This instructs Tenable.io to ignore case.</td>
</tr>
</tbody>
</table>

### equivalent to Scans > Credentials > Plaintext Authentication > telnet/ssh/reexec

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform patch audits over telnet</td>
<td>Disabled</td>
<td>Tenable.io uses telnet to connect to the host device for patch audits.</td>
</tr>
<tr>
<td>Perform patch audits over rsh</td>
<td>Disabled</td>
<td>Tenable.io uses rsh to connect to the host device for patch audits.</td>
</tr>
<tr>
<td>Perform patch audits over rexec</td>
<td>Disabled</td>
<td>Tenable.io uses rexec to connect to the host device for patch audits.</td>
</tr>
</tbody>
</table>

### Windows
<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never send credentials in the clear</td>
<td>Enabled</td>
<td>By default, for security reasons, this option is enabled.</td>
</tr>
<tr>
<td>Do not use NTLMv1 authentication</td>
<td>Enabled</td>
<td>If the <strong>Do not use NTLMv1 authentication</strong> option is disabled, then it is theoretically possible to trick Tenable.io into attempting to log into a Windows server with domain credentials via the NTLM version 1 protocol. This provides the remote attacker with the ability to use a hash obtained from Tenable.io. This hash can be potentially cracked to reveal a username or password. It may also be used to directly log into other servers. Force Tenable.io to use NTLMv2 by enabling the <strong>Only use NTLMv2</strong> setting at scan time. This prevents a hostile Windows server from using NTLM and receiving a hash. Because NTLMv1 is an insecure protocol, this option is enabled by default.</td>
</tr>
<tr>
<td>Start the Remote Registry service during the scan</td>
<td>Disabled</td>
<td>This option tells Tenable.io to start the Remote Registry service on computers being scanned if it is not running. This service must be running in order for Tenable.io to execute some Windows local check plugins.</td>
</tr>
<tr>
<td>Enable administrative shares during the scan</td>
<td>Disabled</td>
<td>This option allows Tenable.io to access certain registry entries that can be read with administrator privileges.</td>
</tr>
</tbody>
</table>

**Note:** This option is disabled by default to improve default scan performance. Additionally, enabling this option can have implications depending on your network security implementation. For example, certain access control configurations for your network firewall might blacklist your scanner for attempting to negotiate Server Message Block Protocol (SMB protocol) connections.
have implications depending on your network security implementation. For example, certain access control configurations for your network firewall might blacklist your scanner for attempting to negotiate Server Message Block Protocol (SMB protocol) connections.

**SSH**

*equivalent to Scans > Credentials > Host > SSH*

|known_hosts file|None|If you upload an SSH known_hosts file, Tenable.io only attempts to log in to hosts in this file. This can ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a log into a system that may not be under your control. |
|Preferred port|22|The port on which SSH is running on the target system. |
|Client version|OpenSSH_5.0|The type of SSH client Tenable.io impersonates while scanning. |
|Attempt least privilege|Cleared|Enables or disables dynamic privilege escalation. When enabled, Tenable.io attempts to run the scan with an account with lesser privileges, even if the Elevate privileges with option is enabled. If a command fails, Tenable.io escalates privileges. Plugins 101975 and 101976 report which plugins ran with or without escalated privileges. |

*Note:* Enabling this option may increase scan run time by up to 30%.

**Amazon AWS**

*equivalent to Scans > Credentials > Cloud Services > Amazon AWS*

|Regions to access|Rest of the World|In order for Tenable.io to audit an Amazon AWS account, you must define the regions you want to scan. Per Amazon policy, you need different credentials to access the Rest of the World. |
audit account configuration for the China region than you do for the rest of the world.

Possible regions include:

- **GovCloud** – If you select this region, you automatically select the government cloud (e.g., us-gov-west-1).

- **Rest of the World** – If you select this region, the following additional options appear:
  - us-east-1
  - us-east-2
  - us-west-1
  - us-west-2
  - ca-central-1
  - eu-west-1
  - eu-west-2
  - eu-central-1
  - ap-northeast-1
  - ap-northeast-2
  - ap-southeast-1
  - ap-southeast-2
  - sa-east-1

- **China** – If you select this region, the following additional options appear:
  - cn-north-1
  - cn-northwest-1
| **HTTPS** | Enabled | Whether Tenable.io authenticates over an encrypted (HTTPS) or an unencrypted (HTTP) connection. |
|**Verify SSL Certificate** | Enabled | Whether Tenable.io verifies the validity of the SSL digital certificate. |

### Rackspace

*equivalent to Scans > Credentials > Cloud Services > Rackspace*

| Location | - | Location of the Rackspace Cloud instance. Possible locations include:  
- Dallas-Fort Worth (DFW)  
- Chicago (ORD)  
- Northern Virginia (IAD)  
- London (LON)  
- Sydney (SYD)  
- Hong Kong (HKG) |

### Microsoft Azure

*equivalent to Scans > Credentials > Cloud Services > Amazon AWS*

| Subscription IDs | - | List subscription IDs to scan, separated by a comma. If this field is blank, all subscriptions are audited. |

### Apple Profile Manager

*equivalent to Scans > Credentials > Mobile > Apple Profile Manager*

| Force device updates | Enabled | Force devices to update with Apple Profile Manager immediately. |
| Device update timeout (minutes) | 5 | Number of minutes to wait for devices to reconnect with Apple Profile Manager. |
Discovery Settings (Classic Interface)

**Note:** If a scan is based on a policy, you cannot configure *Discovery* settings in the scan. You can only modify these settings in the related policy.

The *Discovery* settings relate to discovery and port scanning, including port ranges and methods.

Certain Tenable-provided scanner templates include *preconfigured discovery settings*.

If you select the *Custom* preconfigured setting option, or if you are using a scanner template that does not include preconfigured discovery settings, you can manually configure *Discovery* settings in the following categories:

- **Host Discovery**
- **Port Scanning**
- **Service Discovery**

**Note:** The following tables include settings for the *Advanced Network Scan* template. Depending on the template you select, certain settings may not be available, and default values may vary.

### Host Discovery

**Video:** Advanced Host Discovery Scan Options in Tenable.io

By default, some settings in the *Host Discovery* section are enabled. When you first access the *Host Discovery* section, the *Ping the remote host* item appears and is set to *On*.

The *Host Discovery* section includes the following groups of settings:

- **General Settings**
- **Ping Methods**
- **Fragile Devices**
- **Wake-on-LAN**
- **Network Type**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
<table>
<thead>
<tr>
<th>Value</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping the remote host</td>
<td>On</td>
<td>If set to On, the scanner pings remote hosts on multiple ports to determine if they are alive. Additional options <strong>General Settings</strong> and <strong>Ping Methods</strong> appear. If set to Off, the scanner does not ping remote hosts on multiple ports during the scan.</td>
</tr>
<tr>
<td>Scan unresponsive hosts</td>
<td>Disabled</td>
<td>Specifies whether the Nessus scanner scans hosts that do not respond to any ping methods. This option is only available for scans using the <strong>PCI Quarterly External Scan</strong> template.</td>
</tr>
<tr>
<td>General Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use Fast Network Discovery</td>
<td>Disabled</td>
<td>When disabled, if a host responds to ping, Tenable.io attempts to avoid false positives, performing additional tests to verify the response did not come from a proxy or load balancer. These checks can take some time, especially if the remote host is firewalled. When enabled, Tenable.io does not perform these checks.</td>
</tr>
<tr>
<td>Ping Methods</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ARP</td>
<td>Enabled</td>
<td>Ping a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.</td>
</tr>
<tr>
<td>TCP</td>
<td>Enabled</td>
<td>Ping a host using TCP.</td>
</tr>
<tr>
<td>Destination ports</td>
<td>built-in</td>
<td>Destination ports can be configured to use spe-</td>
</tr>
<tr>
<td>TCP</td>
<td>Specific ports for TCP ping. This specifies the list of ports that are checked via TCP ping. Type one of the following: built-in, a single port, or a comma-separated list of ports. For more information about which ports built-in specifies, see the knowledge base article.</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>ICMP</td>
<td>Enabled</td>
<td>Ping a host using the Internet Control Message Protocol (ICMP).</td>
</tr>
<tr>
<td>Assume ICMP unreachable from the gateway means the host is down</td>
<td>Disabled</td>
<td>Assume ICMP unreachable from the gateway means the host is down. When a ping is sent to a host that is down, its gateway may return an ICMP unreachable message. When this option is enabled, when the scanner receives an ICMP Unreachable message, it considers the targeted host dead. This approach helps speed up discovery on some networks.</td>
</tr>
<tr>
<td>Note: Some firewalls and packet filters use this same behavior for hosts that are up, but connected to a port or protocol that is filtered. With this option enabled, this leads to the scan considering the host is down when it is indeed up.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum number of Retries</td>
<td>2</td>
<td>Specifies the number of attempts to retry pinging the remote host.</td>
</tr>
</tbody>
</table>
| UDP | Disabled | Ping a host using the User Datagram Protocol (UDP). Ping a host using the User Datagram Protocol (UDP). UDP is a stateless protocol, meaning that communication is not performed with handshake dialogues. UDP-based communication is not always reliable, and because of the nature
of UDP services and screening devices, they are not always remotely detectable.

<table>
<thead>
<tr>
<th><strong>Fragile Devices</strong></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Network Printers</strong></td>
<td>Disabled</td>
<td>When enabled, the scanner scans network printers.</td>
</tr>
<tr>
<td><strong>Scan Novell Netware hosts</strong></td>
<td>Disabled</td>
<td>When enabled, the scanner scans Novell NetWare hosts.</td>
</tr>
</tbody>
</table>
| **Scan Operational Technology devices** | Disabled | When enabled, the scanner performs a full scan of Operational Technology (OT) devices such as programmable logic controllers (PLCs) and remote terminal units (RTUs) that monitor environmental factors and the activity and state of machinery.  
When disabled, the scanner uses ICS/SCADA Smart Scanning to cautiously identify OT devices and stops scanning them once they are discovered. |

<table>
<thead>
<tr>
<th><strong>Wake-on-LAN</strong></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| **List of MAC Addresses** | None | The Wake-on-LAN (WOL) menu controls which hosts to send WOL magic packets to before performing a scan.  
Hosts that you want to start prior to scanning are provided by uploading a text file that lists one MAC address per line.  
For example: |

```
33:24:4C:03:CC:C7
FF:5C:2C:71:57:79
```
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot time wait (in minutes)</td>
<td>5 minutes</td>
<td>The amount of time to wait for hosts to start before performing the scan.</td>
</tr>
<tr>
<td>Network Type</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Network Type                  | Mixed (use RFC 1918) | Specifies if you are using publicly routable IPs, private non-Internet routable IPs, or a mix of these. This setting has three options:  
- **Mixed (use RFC 1918)**  
- **Private LAN**  
- **Public WAN (Internet)**  
The default value, **Mixed**, should be selected if you are using RFC 1918 addresses and have multiple routers within your network. |

**Port Scanning**

The **Port Scanning** section includes settings that define how the port scanner behaves and which ports to scan.

The **Port Scanning** section includes the following groups of settings:

- **Ports**
- **Local Port Enumerators**
- **Network Port Scanners**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Consider Unscanned | Disabled     | When enabled, if a port is not scanned with a selected port scanner (for example, the port falls outside of the specified
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports as Closed</td>
<td></td>
<td>the scanner considers it closed.</td>
</tr>
<tr>
<td>Port Scan Range</td>
<td>Default</td>
<td>Specifies the range of ports to be scanned. Supported keyword values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- default instructs the scanner to scan approximately 4,790 commonly used ports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- all instructs the scanner to scan all 65,536 ports, including port 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Additionally, you can indicate a custom list of ports by using a comma-delimited list of ports or port ranges. For example, 21, 23, 25, 80, 110 or 1-1024, 8080, 9000-9200.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you wanted to scan all ports excluding port 0, you would type 1-65535.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The custom range specified for a port scan is applied to the protocols you have selected in the <strong>Network Port Scanners</strong> group of settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If scanning both TCP and UDP, you can specify a split range specific to each protocol. For example, if you want to scan a different range of ports for TCP and UDP in the same policy, you would type T:1-1024,U:300-500.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can also specify a set of ports to scan for both protocols, as well as individual ranges for each separate protocol. For example, 1-1024,T:1024-65535,U:1025.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can also include default in a list of custom ports. For example, T:64999,default,U:55550-55555.</td>
</tr>
</tbody>
</table>

**Local Port Enumerators**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH (netstat)</td>
<td>Enabled</td>
<td>When enabled, the scanner uses netstat to check for open ports.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| WMI (netstat)               | Enabled       | When enabled, the scanner uses netstat to determine open ports while performing a WMI-based scan. In addition, the scanner:  
|                             |               |   - Ignores any custom range specified in the **Port Scan Range** setting.  
|                             |               |   - Continues to treat unscanned ports as closed if the **Consider unscanned ports as closed** setting is enabled.  
<p>|                             |               | If any port enumerator (netstat or SNMP) is successful, the port range becomes <em>all</em>.                                                                                                                        |
| SNMP                        | Enabled       | When enabled, if the appropriate credentials are provided by the user, the scanner can better test the remote host and produce more detailed audit results. For example, there are many Cisco router checks that determine the vulnerabilities present by examining the version of the returned SNMP string. This information is necessary for these audits. |
| Only run network port scanners if local port enumeration failed | Enabled       | When enabled, the scanner relies on local port enumeration first before relying on network port scans.                                                                                                       |
| Verify open TCP             | Disabled      | When enabled, if a local port enumerator (for example, netstat or SNMP) is successful, the port range becomes <em>all</em>.                                                                                           |</p>
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ports found by local port enumerators</td>
<td></td>
<td>WMI or netstat) finds a port, the scanner also verifies that the port is open remotely. This approach helps determine if some form of access control is being used (for example, TCP wrappers or a firewall).</td>
</tr>
<tr>
<td><strong>Network Port Scanners</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>Disabled</td>
<td>Use the built-in Nessus TCP scanner to identify open TCP ports on the targets, using a full TCP three-way handshake. TCP scans are only possible if you are using Linux or FreeBSD. On Windows or Mac OS X, the scanner does not do a TCP scan and instead uses the SYN scanner to avoid performance issues native to those operating systems. If you enable this option, you can also set the <strong>Override Automatic Firewall Detection</strong> option.</td>
</tr>
<tr>
<td>Override automatic firewall detection</td>
<td>Disabled</td>
<td>This setting can be enabled if you enable either the <strong>TCP</strong> or <strong>SYN</strong> option. When enabled, this setting overrides automatic firewall detection. This setting has three options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Use aggressive detection</strong> attempts to run plugins even if the port appears to be closed. It is recommended that this option not be used on a production network.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Use soft detection</strong> disables the ability to monitor how often resets are set and to determine if there is a limitation configured by a downstream network device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Disable detection</strong> disables the firewall detection feature.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This description also applies to the <strong>Override automatic firewall detection</strong> setting that is available following SYN.</td>
</tr>
<tr>
<td>SYN</td>
<td>Enabled</td>
<td>Use the built-in Nessus SYN scanner to identify open TCP ports on the target hosts. SYN scans do not initiate a full TCP three-way handshake. The scanner sends a SYN packet to the port, waits for SYN-ACK reply, and determines the port state based on a response or lack of response. If you enable this option, you can also set the <strong>Override Automatic Firewall Detection</strong> option.</td>
</tr>
<tr>
<td>UDP</td>
<td>Disabled</td>
<td>This option engages the built-in Nessus UDP scanner to identify open UDP ports on the targets. Due to the nature of the protocol, it is generally not possible for a port scanner to tell the difference between open and filtered UDP ports. Enabling the UDP port scanner may dramatically increase the scan time and produce unreliable results. Consider using the netstat or SNMP port enumeration options instead if possible.</td>
</tr>
</tbody>
</table>

**Service Discovery**

The **Service Discovery** section includes settings that attempt to map each open port with the service that is running on that port.

The **Service Discovery** section includes the following groups of settings:

- [General Settings](#)
- [Search for SSL/TLS Services](#)
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Probe all ports to find services</td>
<td>Enabled</td>
<td>Attempts to map each open port with the service that is running on that port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Caution:</strong> In some rare cases, probing might disrupt some services and cause unforeseen side effects.</td>
</tr>
<tr>
<td>Search for SSL based services</td>
<td>On</td>
<td>Controls how Tenable.io will test SSL-based services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Caution:</strong> Testing for SSL capability on all ports may be disruptive for the tested host.</td>
</tr>
<tr>
<td>Search for SSL/TLS Services (enabled)</td>
<td></td>
<td>This setting has two options:</td>
</tr>
<tr>
<td>Search for SSL/TLS on</td>
<td>Known SSL/TLS ports</td>
<td></td>
</tr>
<tr>
<td></td>
<td>60</td>
<td>Identifies SSL and TLS certificates that are within the specified number of days of expiring.</td>
</tr>
<tr>
<td>Identify certificates expiring within x days</td>
<td>True</td>
<td>When enabled, Tenable.io ignores the list of ciphers advertised by SSL/TLS services and enumerates them by attempting to establish connections using all possible ciphers.</td>
</tr>
<tr>
<td>Enumerate all SSL ciphers</td>
<td>True</td>
<td>When enabled, Tenable.io checks that none of the identified certificates have been revoked.</td>
</tr>
<tr>
<td>Enable CRL checking (connects to Internet)</td>
<td>False</td>
<td></td>
</tr>
</tbody>
</table>
Assessment Settings (Classic Interface)

**Note:** If a scan is based on a policy, you cannot configure Assessment settings in the scan. You can only modify these settings in the related policy.

You can use Assessment settings to configure how a scan identifies vulnerabilities, as well as what vulnerabilities are identified. This includes identifying malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility of web applications.

Certain Tenable-provided scanner templates include preconfigured assessment settings.

If you select the Custom preconfigured setting option, or if you are using a scanner template that does not include preconfigured assessment settings, you can manually configure Assessment settings in the following categories:

- **General**
- **Brute Force**
- **SCADA**
- **Web Applications**
- **Windows**
- **Malware**

**Note:** The following tables include settings for the Advanced Network Scan template. Depending on the template you select, certain settings may not be available, and default values may vary.

### General

The General section includes the following groups of settings:

- **Accuracy**
- **Antivirus**
- **SMTP**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
</table>

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable,Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
### Accuracy

| Override normal Accuracy | Disabled | In some cases, Tenable.io cannot remotely determine whether a flaw is present or not. If report paranoia is set to **Show potential false alarms**, a flaw is reported every time, even when there is a doubt about the remote host being affected. Conversely, a paranoia setting of **Avoid potential false alarms** causes Tenable.io to not report any flaw whenever there is a hint of uncertainty about the remote host. As a middle ground between these two settings, disable this setting. |

| Perform thorough tests (may disrupt your network or impact scan speed) | Disabled | Causes various plugins to work harder. For example, when looking through SMB file shares, a plugin analyzes 3 directory levels deep instead of 1. This could cause much more network traffic and analysis in some cases. By being more thorough, the scan is more intrusive and is more likely to disrupt the network, while potentially providing better audit results. |

### Antivirus

| Antivirus definition grace period (in days) | 0 | Configure the delay of the Antivirus software check for a set number of days (0-7). The Antivirus Software Check menu allows you to direct Tenable.io to allow for a specific grace time in reporting when antivirus signatures are considered out of date. By default, Tenable.io considers signatures out of date regardless of how long ago an update became available (e.g., a few hours ago). You can configure this option to allow for up to 7 days before reporting them out of date. |

### SMTP

| Third party domain | Tenable.io attempts to send spam through each SMTP device to the address listed in this field. This third party domain address must be outside the range of |
the site being scanned or the site performing the scan. Otherwise, the test may be aborted by the SMTP server.

<table>
<thead>
<tr>
<th>From address</th>
<th>The test messages sent to the SMTP server(s) appear as if the messages originated from the address specified in this field.</th>
</tr>
</thead>
<tbody>
<tr>
<td>To address</td>
<td>Tenable.io attempts to send messages addressed to the mail recipient listed in this field. The postmaster address is the default value since it is a valid address on most mail servers.</td>
</tr>
</tbody>
</table>

**Brute Force**

The **Brute Force** section includes the following groups of settings:

- General Settings
- Oracle Database

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Only use credentials provided by the user</td>
<td>Enabled</td>
<td>In some cases, Tenable.io can test default accounts and known default passwords. This can cause the account to be locked out if too many consecutive invalid attempts trigger security protocols on the operating system or application. By default, this setting is enabled to prevent Tenable.io from performing these tests.</td>
</tr>
<tr>
<td>Oracle Database</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test default accounts (slow)</td>
<td>Disabled</td>
<td>Test for known default accounts in Oracle software.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Modbus/TCP Coil Access</td>
<td></td>
<td>Modbus uses a function code of 1 to read coils in a Modbus slave. Coils represent binary output settings and are typically mapped to actuators. The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a write coil message.</td>
</tr>
<tr>
<td>Start at Register</td>
<td>0</td>
<td>The register at which to start scanning.</td>
</tr>
<tr>
<td>End at Register</td>
<td>16</td>
<td>The register at which to stop scanning.</td>
</tr>
<tr>
<td>ICCP/COTP TSAP</td>
<td></td>
<td>The ICCP/COTP TSAP Addressing menu determines a Connection Oriented Transport Protocol (COTP) Transport Service Access Points (TSAP) value on an ICCP server by trying possible values.</td>
</tr>
<tr>
<td>Start COTP TSAP</td>
<td>8</td>
<td>Specifies the starting TSAP value to try. Tenable.io tries all values between the Start and Stop values.</td>
</tr>
<tr>
<td>Stop COTP TSAP</td>
<td>8</td>
<td>Specifies the ending TSAP value to try. Tenable.io tries all values between the Start and Stop values.</td>
</tr>
</tbody>
</table>

**Web Applications**

By default, Tenable.io does not scan web applications. When you first access the Web Application section, the Scan Web Applications setting appears and is set to Off. To modify the Web Application settings listed on the following table, click the Off button. The rest of the settings appear.

The **Web Applications** section includes the following groups of settings:

- **General Settings**
- **Web Crawler**
- **Application Test Settings**
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use the cloud to take screenshots of public</td>
<td>Disabled</td>
<td>This option enables Tenable.io to take screenshots to better demonstrate some findings. This includes some services (e.g., VNC, RDP) as well as configuration specific options (e.g., web server directory indexing). The feature only works for Internet-facing hosts, as the screenshots are generated on a managed server and sent to the Tenable.io scanner. Tenable.io does not export screenshots with Tenable.io scan reports.</td>
</tr>
<tr>
<td>webservers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use a custom User-Agent</td>
<td>Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)</td>
<td>Specifies which type of web browser Tenable.io impersonates while scanning.</td>
</tr>
<tr>
<td><strong>Web Crawler</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start crawling from</td>
<td>/</td>
<td>The URL of the first page that is tested. If multiple pages are required, use a colon delimiter to separate them (e.g., /:/php-p4:/base).</td>
</tr>
<tr>
<td>Excluded pages (regex)</td>
<td>/server_privileges.php</td>
<td>log out</td>
</tr>
</tbody>
</table>

---

**Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable,Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.**
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum pages to crawl</td>
<td>1000</td>
<td>The maximum number of pages to crawl.</td>
</tr>
<tr>
<td>Maximum depth to crawl</td>
<td>6</td>
<td>Limit the number of links Tenable.io follows for each start page.</td>
</tr>
<tr>
<td>Follow dynamically generated</td>
<td>Disabled</td>
<td>If selected, Tenable.io follows dynamic links and may exceed the parameters set above.</td>
</tr>
<tr>
<td>pages</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Application Test Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable generic web application tests</td>
<td>Disabled</td>
<td>Enables the options listed below.</td>
</tr>
<tr>
<td>Abort web application tests if HTTP login fails</td>
<td>Disabled</td>
<td>If Tenable.io cannot log in to the target via HTTP, then do not run any web application tests.</td>
</tr>
<tr>
<td>Try all HTTP methods</td>
<td>Disabled</td>
<td>This option instructs Tenable.io to also use POST requests for enhanced web form testing. By default, the web application tests only use GET requests, unless you enable this option. Generally, more complex applications use the POST method when a user submits data to the application. When enabled, Tenable.io tests each script or variable with both GET and POST requests. This setting provides more thorough testing, but may considerably increase the time required.</td>
</tr>
<tr>
<td>Attempt HTTP Parameter Policy</td>
<td>Disabled</td>
<td>When performing web application tests,</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>lution</td>
<td></td>
<td>attempt to bypass filtering mechanisms by injecting content into a variable while also supplying the same variable with valid content. For example, a normal SQL injection test may look like /target.cgi?a=&amp;b=2. With HTTP Parameter Pollution (HPP) enabled, the request may look like /target.cgi?a=&amp;a=1&amp;b=2.</td>
</tr>
<tr>
<td>Test embedded web servers</td>
<td>Disabled</td>
<td>Embedded web servers are often static and contain no customizable CGI scripts. In addition, embedded web servers may be prone to crash or become non-responsive when scanned. Tenable recommends scanning embedded web servers separately from other web servers using this option.</td>
</tr>
</tbody>
</table>
| Test more than one parameter at a time perform | Disabled      | This setting manages the combination of argument values used in the HTTP requests. The default, without checking this option, is testing one parameter at a time with an attack string, without trying non-attack variations for additional parameters. For example, Tenable.io would attempt /test.php?arg1=XSS&b=1&c=1, where b and c allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated. This setting has four options:  
  - **Test random pairs of parameters:**  
    This form of testing randomly checks |
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>a combination of random pairs of parameters. This is the fastest way to test multiple parameters.</td>
</tr>
</tbody>
</table>

- **Test all pairs of parameters (slow):** This form of testing is slightly slower but more efficient than the one value test. While testing multiple parameters, it tests an attack string, variations for a single variable and then use the first value for all other variables. For example, Tenable.io would attempt /test.php?a=a=XSS&b=1&c=1&d=1 and then cycle through the variables so that one is given the attack string, one is cycled through all possible values (as discovered during the mirror process) and any other variables are given the first value. In this case, Tenable.io would never test for /test.php?a=a=XSS&b=3&c=3&d=3 when the first value of each variable is 1.

- **Test random combinations of three or more parameters (slower):** This form of testing randomly checks a combination of three or more parameters. This is more thorough than testing only pairs of parameters. Increasing the amount of combinations by three or more increases the web application test time.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test all combinations of parameters (slowest):</td>
<td></td>
<td>• <strong>Test all combinations of parameters (slowest):</strong> This method of testing checks all possible combinations of attack strings with valid input to variables. Where all pairs testing seeks to create a smaller data set as a tradeoff for speed, all combinations makes no compromise on time and uses a complete data set of tests. This testing method may take a long time to complete.</td>
</tr>
<tr>
<td>Do not stop after first flaw is found per web page</td>
<td>Disabled</td>
<td>This setting determines when to target a new flaw. This applies at the script level. Finding an XSS flaw does not disable searching for SQL injection or header injection, but unless otherwise specified, there is at most one report for each type on a given port. Note that several flaws of the same type (e.g., XSS, SQLi, etc.) may be reported if the flaws were caught by the same attack. This setting has three options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Stop after one flaw is found per web server (fastest):</strong> As soon as a flaw is found on a web server by a script, Tenable.io stops and switches to another web server on a different port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Stop after one flaw is found per parameter (slow):</strong> As soon as one parameter...</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Type of flaw is found in a parameter of a CGI (e.g., XSS), Tenable.io switches to the next parameter of the same CGI, the next known CGI, or to the next port or server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Look for all flaws (slowest):</td>
<td></td>
<td>Perform extensive tests regardless of flaws found. This option can produce a very verbose report and is not recommend in most cases.</td>
</tr>
<tr>
<td>URL for Remote File Inclusion</td>
<td><a href="http://rfi.nessus.org/rfi.txt">http://rfi.nessus.org/rfi.txt</a></td>
<td>During Remote File Inclusion (RFI) testing, this setting specifies a file on a remote host to use for tests. By default, Tenable.io uses a safe file hosted by Tenable for RFI testing. If the scanner cannot reach the Internet, you can use an internally hosted file for more accurate RFI testing.</td>
</tr>
<tr>
<td>Maximum run time (min)</td>
<td>5</td>
<td>This option manages the amount of time in minutes spent performing web application tests. This option defaults to 60 minutes and applies to all ports and CGIs for a given website. Scanning the local network for web sites with small applications typically completes in under an hour, however web sites with large applications may require a higher value.</td>
</tr>
</tbody>
</table>

Windows

The Windows section contains the following groups of settings:
- **General Settings**

- **User Enumeration Methods**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request information about the SMB Domain</td>
<td>Disabled</td>
<td>If enabled, domain users are queried instead of local users.</td>
</tr>
<tr>
<td><strong>User Enumeration Methods</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>You can enable as many of the user enumeration methods as appropriate for user discovery.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAM Registry</td>
<td>Enabled</td>
<td>Tenable.io enumerates users via the Security Account Manager (SAM) registry.</td>
</tr>
<tr>
<td>ADSI Query</td>
<td>Enabled</td>
<td>Tenable.io enumerates users via Active Directory Service Interfaces (ADSI). To use ADSI, you must configure credentials under <strong>Credentials &gt; Miscellaneous &gt; ADSI</strong>.</td>
</tr>
<tr>
<td>WMI Query</td>
<td>Enabled</td>
<td>Tenable.io enumerates users via Windows Management Interface (WMI).</td>
</tr>
<tr>
<td>RID Brute Forcing</td>
<td>Disabled</td>
<td>Tenable.io enumerates users via relative identifier (RID) brute forcing. Enabling this setting enables the <strong>Enumerate Domain Users</strong> and <strong>Enumerate Local User</strong> settings.</td>
</tr>
</tbody>
</table>

**Enumerate Domain Users (available with RID Brute Forcing enabled)**

| Start UID | 1000 | The beginning of a range of IDs where Tenable.io attempts to enumerate domain users. |
| End UID   | 1200 | The end of a range of IDs where Tenable.io attempts to enumerate domain users.     |

**Enumerate Local User (available with RID Brute Forcing enabled)**
Malware

The Malware section contains the following groups of settings:

- **General Settings**
- **Hash and Whitelist Files**
- **File System Scanning**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disable DNS resolution</td>
<td>Disabled</td>
<td>Checking this option prevents Tenable.io from using the cloud to compare scan findings against known malware.</td>
</tr>
<tr>
<td>Hash and Whitelist Files</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom Netstat IP Threat List</td>
<td>None</td>
<td>A text file that contains a list of known bad IP addresses that you want to detect. Each line in the file must begin with an IPv4 address. Optionally, you can add a description by adding a comma after the IP address, followed by the description. You can also use hash-delimited comments (e.g., #) in addition to comma-delimited comments.</td>
</tr>
<tr>
<td>Provide your own list of known bad MD5 hashes</td>
<td>None</td>
<td>A text file with one MD5 hash per line that specifies additional known bad MD5 hashes. Optionally, you can include a description for a hash by...</td>
</tr>
<tr>
<td>Feature</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Provide your own list of known good MD5 hashes</td>
<td>None</td>
<td>A text file with one MD5 hash per line that specifies additional known good MD5 hashes. Optionally, you can include a description for each hash by adding a comma after the hash, followed by the description. If any matches are found when scanning a target, and a description was provided for the hash, the description appears in the scan results. You can also use hash-delimited comments (e.g., #) in addition to comma-delimited comments.</td>
</tr>
<tr>
<td>Hosts file whitelist</td>
<td>None</td>
<td>Tenable.io checks system hosts files for signs of a compromise (e.g., Plugin ID 23910 titled Compromised Windows System (hosts File Check)). This option allows you to upload a file containing a list of IPs and hostnames you want Tenable.io to ignore during a scan. Include one IP and one hostname (formatted identically to your hosts file on the target) per line in a regular text file.</td>
</tr>
</tbody>
</table>

**File System Scanning**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan file system</td>
<td>Off</td>
<td>If enabled, Tenable.io can scan system directories and files on host computers.</td>
</tr>
<tr>
<td>Scan %Systemroot%</td>
<td>Off</td>
<td>Enables file system scanning to scan %Systemroot%.</td>
</tr>
<tr>
<td>Scan %Pro-</td>
<td>Off</td>
<td>Enables file system scanning to scan %Pro-</td>
</tr>
<tr>
<td>Feature</td>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Scan %ProgramFiles (x86)%</td>
<td>Off</td>
<td>Enables file system scanning to scan %ProgramFiles (x86)%.</td>
</tr>
<tr>
<td>Scan %ProgramData%</td>
<td>Off</td>
<td>Enables file system scanning to scan %ProgramData%.</td>
</tr>
<tr>
<td>Scan User Profiles</td>
<td>Off</td>
<td>Enables file system scanning to scan user profiles.</td>
</tr>
<tr>
<td>Custom Filescan Directories</td>
<td>None</td>
<td>A custom file that lists directories to be scanned by malware file scanning. List each directory on one line.</td>
</tr>
<tr>
<td>Yara Rules File</td>
<td>None</td>
<td>A .yar file containing the YARA rules to be applied in the scan. You can only upload one file per scan, so include all rules in a single file. For more information, see <a href="https://yara.readthedocs.io">yara.readthedocs.io</a>.</td>
</tr>
</tbody>
</table>
**Report Settings (Classic Interface)**

The Report settings include the following groups of settings:

- **Processing**
- **Output**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Override normal verbosity</td>
<td>Disabled</td>
<td>This setting has two options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>I have limited disk space. Report as little information as possible:</strong> Provides less information about plugin activity in the report to minimize impact on disk space.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Report as much information as possible:</strong> Provides more information about plugin activity in the report.</td>
</tr>
<tr>
<td>Show missing patches that have been superseded</td>
<td>Enabled</td>
<td>If enabled, includes superseded patch information in the scan report.</td>
</tr>
<tr>
<td>Hide results from plugins initiated as a dependency</td>
<td>Enabled</td>
<td>If enabled, the list of dependencies is not included in the report. If you want to include the list of dependencies in the report, disable this setting.</td>
</tr>
<tr>
<td>Output</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow users to edit scan results</td>
<td>Enabled</td>
<td>When enabled, allows users to delete items from the report. When performing a scan for regulatory compliance or other types of audits, disable the setting to show that the scan was not tampered with.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Designate hosts by their DNS name</td>
<td>Disabled</td>
<td>Uses the hostname rather than IP address for report output.</td>
</tr>
<tr>
<td>Display hosts that respond to ping</td>
<td>Disabled</td>
<td>Reports hosts that successfully respond to a ping.</td>
</tr>
<tr>
<td>Display unreachable hosts</td>
<td>Disabled</td>
<td>When enabled, hosts that did not reply to the ping request are included in the security report as dead hosts. Do not enable this option for large IP blocks.</td>
</tr>
</tbody>
</table>
The **Advanced** settings provide increased control over scan efficiency and the operations of a scan, as well as the ability to enable plugin debugging.

Certain Tenable-provided scanner templates include **preconfigured advanced settings**.

If you select the **Custom** preconfigured setting option, or if you are using a scanner template that does not include preconfigured advanced settings, you can manually configure **Advanced** settings in the following categories:

- **General Settings**
- **Performance**
- **Debug Settings**

**Note:** The following tables include settings for the **Advanced Network Scan** template. Depending on the template you select, certain settings may not be available, and default values may vary.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Safe Checks</td>
<td>Enabled</td>
<td>When enabled, disables all plugins that may have an adverse effect on the remote host.</td>
</tr>
<tr>
<td>Stop scanning hosts that become unresponsive during the scan</td>
<td>Disabled</td>
<td>When enabled, Tenable.io stops scanning if it detects that the host has become unresponsive. This may occur if users turn off their PCs during a scan, a host has stopped responding after a denial of service plugin, or a security mechanism (for example, an IDS) has started to block traffic to a server. Normally, continuing scans on these machines sends unnecessary traffic across the network and delay the scan.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Scan IP addresses in a random order</td>
<td>Disabled</td>
<td>By default, Tenable.io scans a list of IP addresses in sequential order. When this option is enabled, Tenable.io scans the list of hosts in a random order within an IP address range. This approach is typically useful in helping to distribute the network traffic during large scans.</td>
</tr>
<tr>
<td>Scan targets with multiple domain names in parallel</td>
<td>Disabled</td>
<td>When disabled, to avoid overwhelming a host, Tenable.io prevents a single scanner from Nessus preventing against simultaneously scanning multiple targets that resolve to a single IP address. Instead, Tenable.ioNessus scanners serialize attempts to scan the IP address, whether it appears more than once in the same scan task or in multiple scan tasks on that scanner. Scans may take longer to complete. When enabled, a Tenable.ioNessus scanner can simultaneously scan multiple targets that resolve to a single IP address within a single scan task or across multiple scan tasks. Scans complete more quickly, but hosts could potentially become overwhelmed, causing timeouts and incomplete results.</td>
</tr>
<tr>
<td>Automatically accept detected SSH disclaimer prompts</td>
<td>Disabled</td>
<td>When enabled, if a credentialed scan tries to connect via SSH to a FortiOS host that presents a disclaimer prompt, the scanner provides the necessary text input to accept the disclaimer prompt and continue the scan. When disabled, credentialed scans on hosts that present a disclaimer prompt fail because the scanner cannot connect to the device and accept the disclaimer. The error appears in the plugin output.</td>
</tr>
<tr>
<td>Create unique identifier on</td>
<td>Enabled</td>
<td>When enabled, the scanner creates a unique identifier for credentialed scans.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>hosts scanned using credentials</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Performance Options</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slow down the scan when network congestion is detected</td>
<td>Disabled</td>
<td>When enabled, Tenable.io detects when it is sending too many packets and the network pipe is approaching capacity. If network congestion is detected, Tenable.io throttles the scan to accommodate and alleviate the congestion. Once the congestion has subsided, Tenable.io automatically attempts to use the available space within the network pipe again.</td>
</tr>
<tr>
<td>Use Linux kernel congestion detection</td>
<td>Disabled</td>
<td>This enables Tenable.io to use the Linux kernel to detect when it sends too many packets and the network pipe approaches capacity. If detected, Tenable.io throttles the scan to accommodate and alleviate the congestion. Once the congestion subsides, Tenable.io automatically attempts to use the available space within the network pipe again.</td>
</tr>
<tr>
<td>Network timeout (in seconds)</td>
<td>5</td>
<td>Specifies the time that Tenable.io waits for a response from a host unless otherwise specified within a plugin. If you are scanning over a slow connection, you may want to set this to a higher number of seconds.</td>
</tr>
<tr>
<td>Max simultaneous checks per host</td>
<td>5</td>
<td>Specifies the maximum number of checks a Tenable.io scanner will perform against a single host at one time.</td>
</tr>
<tr>
<td>Max simultaneous hosts per scan</td>
<td>80</td>
<td>Specifies the maximum number of hosts that a Tenable.io scanner will scan at the same time.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Max number of concurrent TCP sessions per host</td>
<td>none</td>
<td>Specifies the maximum number of established TCP sessions for a single host. This TCP throttling option also controls the number of packets per second the SYN scanner sends, which is 10 times the number of TCP sessions. For example, if this option is set to 15, the SYN scanner sends 150 packets per second at most.</td>
</tr>
<tr>
<td>Max number of concurrent TCP sessions per scan</td>
<td>none</td>
<td>Specifies the maximum number of established TCP sessions for the entire scan, regardless of the number of hosts being scanned. For scanners installed on any Windows host, you must set this value to 19 or less to get accurate results.</td>
</tr>
<tr>
<td>Unix find command exclusions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom filepath</td>
<td>none</td>
<td>A plain text file containing a list of filepaths to exclude from all plugins that search using the <code>find</code> command on Unix systems. In the file, enter one_filepath per line, formatted per patterns allowed by the Unix <code>find</code> command <code>-path</code> argument. For more information, see the <code>find</code> command <a href="#">man page</a>.</td>
</tr>
<tr>
<td>Custom filesystem</td>
<td>none</td>
<td>A plain text file containing a list of filesystems to exclude from all plugins that search using the <code>find</code> command on Unix systems. In the file, enter one filestystem per line, using filesystem types supported by the Unix <code>find</code> command <code>-fstype</code> argument. For more information, see the <code>find</code> command <a href="#">man page</a>.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Debug Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable plugin debugging</td>
<td>Disabled</td>
<td>Attaches available debug logs from plugins to the vulnerability output of this scan.</td>
</tr>
<tr>
<td>Audit Trail Verbosity</td>
<td>No audit trail</td>
<td>Controls verbosity of the plugin audit trail. <strong>All audit trail data</strong> includes the reason why plugins were not included in the scan.</td>
</tr>
</tbody>
</table>
You can use credentials to grant the Tenable.io scanner local access to scan the target system without requiring an agent.

Credentialed scans can perform a wider variety of checks than non-credentialed scans, which can result in more accurate scan results. This facilitates scanning of a very large network to determine local exposures or compliance violations.

Credentialed scans can perform any operation that a local user can perform. The level of scanning depends on the privileges granted to the user account. The more privileges the scanner has via the login account (e.g., root or administrator access), the more thorough the scan results.

In Tenable.io, you can create credentials for use in scans in the following ways:

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan-specific</td>
<td>• You configure and store these credentials in an individual scan.</td>
<td>User Permissions in Basic settings in the scan</td>
</tr>
<tr>
<td></td>
<td>• If you delete the scan, you also delete the credentials.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If you want to use the credentials in a different scan, you must either convert the scan-specific credential to a managed credential or recreate the scan-specific credential settings in the other scan.</td>
<td></td>
</tr>
<tr>
<td>Policy-specific</td>
<td>• You configure and store these credentials in a scan policy. You can then use the policy to create individual scans.</td>
<td>User Permissions in Basic settings in the policy</td>
</tr>
<tr>
<td></td>
<td>• If you add credentials to a policy, other users can override those credentials by adding scan-specific or managed credentials to scans created from the</td>
<td></td>
</tr>
</tbody>
</table>
Policy. Tenable recommends adding managed credentials to scans, instead of adding credentials to policies.

- If you delete the policy, you also delete the policy-specific credentials. However, Tenable.io retains the credentials in any scans you used the policy to create before deletion.

- If you want to use the credentials in a different policy, you must recreate the policy-specific credentials in the other policy.

**Managed**

- Tenable.io stores managed credentials centrally in the **credential manager**. You can configure managed credentials directly in the credential manager or during **scan configuration**. You can also convert a scan-specific credential to a managed credential during scan configuration.

- You can use managed credentials in multiple scans. You can also grant other users permissions to use managed credentials in scans.

- You cannot use managed credentials in policies.

The settings you configure for a credential vary based on the credential type. Credential types include:

- **Cloud Services**
- **Database**
- **Host**
- **Miscellaneous**
- **Mobile Device Management**
• **Patch Management**

• ** Plaintext authentication**

**Video:** Simulate Credential Manager Role

**Note:** Tenable.io opens several concurrent authenticated connections. Ensure that the host being audited does not have a strict account lockout policy based on concurrent sessions.

**Note:** By default, when creating credentialed scans or polices, hosts are identified and marked with a [Tenable Asset Identifier (TAI)]#. This globally unique identifier is written to the host's registry or file system, and subsequent scans can retrieve and use the TAI.

This option is enabled (by default) or disabled in the [Advanced -> General Settings] of a scan or policy's configuration settings: **Create unique identifier on hosts scanned using credentials.**
Add or Edit Managed Credentials for a Scan (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can Control

To add or edit a managed credential for a scan:

1. In the top navigation bar, click **Scans**.
   The **My Scans** page appears.

2. Do one of the following:
   - **Create** a new scan
   - **Edit** an existing scan
     a. Click the scan you want to edit
     b. Click **Configure**

3. In the scans table, click the **Credentials** tab.

4. Do one of the following:

**Add an existing managed credential.**

a. In the **Add Managed Credential** section, click **Add**.
   The **Select Credentials to Add to Scan** window appears. This window contains the managed credentials table.

   The managed credentials table contains any credentials where you have **Can Use** or **Can Edit** permissions. For more information, see [Configure User Permissions for a Managed Credential](#).

b. In the managed credentials table, select the check box next to each managed credential you want to add.
c. Click Add.

Convert a scan-specific credential to a managed credential.

**Note:** Only scan owners can convert a scan-specific credential to a managed credential.

A scan-specific credential can only be used in a single scan. To reuse a scan-specific credential in multiple scans, convert it to a managed credential.

a. If adding a new credential, click the credential type in the **Add Credentials** list, then configure the [credential settings](#).

   -or-

   If converting an existing credential, click the credential in the list of credentials assigned to the scan.

b. Click **Save to Managed Credentials**.

c. Enter a name for the managed credential.

d. Click **Save**.

   Tenable.io adds the managed credential and assigns you **Can Edit** user permissions for the credential.

   If you want to add other user permissions, see [Configure User Permissions for a Managed Credential](#).

Edit a managed credential assigned to a scan.

**Note:** You can only view or edit settings for managed credential where you have **Can Edit** permissions.

a. In the list of credentials assigned to the scan, click the credential you want to edit.

   The credential settings appear.

b. Make your changes to the **credential settings**.

c. Click **Apply Changes**.
Tenable.io determines whether any other scans use the managed credential and prompts you to confirm the changes.

d. If you want to save the changes to the managed credential, click **Yes**. Tenable.io saves your changes.

-or-

If you want to cancel the changes you made, click **Cancel**. Tenable.io discards your changes.
Selenium

These steps describe how to create a Selenium script to use with the **Selenium Authentication** option in the **Credentials** settings for the **Web App Overview** and **Web App Scan** templates.

**Tip:** For information about Selenium scripts you can use with WAS, see [WAS Selenium Commands](#).

Before you begin:

- Confirm your application is compatible with Google Chrome. For more information, see [Application Requirements](#).

To use Selenium authentication:

1. Click **Scans** > **New Scan** > **Web Application** > **Web App Scan** or **Web App Overview**.
2. Click the **Credentials** tab.
3. In the **Add Credentials** section, click **Web Application Authentication**.
4. From the **Authentication Method** drop-down box, select **Selenium Authentication**.

5. Optionally, click **Click here to open Chrome Extension** to use the Web App Scanning Google Chrome extension. See [WAS Chrome Extension (Classic Interface)](#) for more information.

6. To use the **Selenium script** section, you must first create a .side file:
   
   a. In Google Chrome, install the **Selenium IDE extension**.
   
   b. For the web application you want to scan, access the login page in Google Chrome.
c. In the upper right corner of the browser window, click the button to launch the Selenium IDE extension.

The Selenium IDE window appears.
d. In the upper right corner of the Selenium IDE window, click the button to begin the recording.

e. On the login page, enter your credentials and submit.

   Selenium IDE captures your actions.

f. Upon successful authentication, in the upper right corner of the Selenium IDE window, click the button to stop the recording.

g. Click the button to save the project.

7. Click Add file and select the .side file created in step 7.

8. In the Page to verify active session text box, type the URL that Tenable.io can continually access to ensure the authenticated session is still valid.
9. In the **Pattern to verify active session** text box, type a word, phrase, or regular expression that appears on the page specified in the **Page to verify active session** text box. This phrase only appears if the authenticated session is still valid.

**Login Form**

To use Login Form authentication:

1. Click **Scans > New Scan > Web Application > Web App Scan** or **Web App Overview**.
2. Click the **Credentials** tab.
3. In the **Add Credentials** section, click **Web Application Authentication**.
4. From the **Authentication Method** drop-down box, select **Login Form**.

5. In the **Login Page** text box, type the URL of the login page for which you wish to attempt authentication.

6. In the **Credentials** section, specify the form field names in the **example: username** and **example: password** text boxes, as well as their respective values in corresponding text boxes to the right.

   **Tip:** When performing an uncredentialed Web App Overview, plugin 98033 (Login Form Detected) may automatically detect the necessary form field names to type in the **example: username** and **example: password** text boxes of the credentials area.

7. In the **Pattern to verify successful auth** text box, type a word, phrase, or regular expression that indicates the login was successful.
8. In the **Page to verify active session** text box, type the URL that Tenable.io can continually access to ensure the authenticated session is still valid.

**Tip:** Tenable recommends including "My Account" or "My Preferences" as part of the URL for the **Page to verify active session** text box.

9. In the **Pattern to verify active session** text box, type a word, phrase, or regular expression that appears on the page specified in the **Page to verify active session** text box. This phrase only appears if the authenticated session is still valid.
Scan Folders (Classic Interface)

The **Folders** section contains all of your configured scans in Tenable.io, organized into folders.

The **Folders** section always includes the following default folders that cannot be removed:

- **My Scans**
- **All Scans**
- **Trash**

By default, when you access the **Scans** page, the **My Scans** folder appears. When you create a scan, it appears in the **My Scans** folder by default. You can then move the scan to a different new or existing folder.

The **All Scans** folder displays all scans you have created as well as any scans that you have permission to interact with.

The **Trash** folder displays scans that you have deleted. In the **Trash** folder, you can permanently remove scans from your Tenable.io instance, or restore the scans to a selected folder. If you delete a folder that contains scans, all scans in that folder are moved to the **Trash** folder. Scans stored in the **Trash** folder are automatically deleted after 30 days.

**Note:** Users with administrative privileges can view all user-created scans in Tenable.io.

For more information, see **Manage Scan Folders (Classic Interface)**.
Manage Scan Folders (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can View

In addition to the Tenable-provided default folders (*All Scans*, *My Scans*, Trash), you can create custom folders for organizing your scans. You are the only user who can view, rename, or delete the custom folders you create. You cannot share the custom folders you create with other users.

You can move a scan from a default folder to either the *My Scans* default folder or a custom scan folder. You can also move a scan from a custom folder to the *My Scans* default folder or a different custom folder.

If you move a scan from the *All Scans* default folder, the scan appears in both the folder you select and the *All Scans* folder.

If you move a scan from the *My Scans* default folder, the scan appears in the custom folder only.

For information about moving a scan to the trash, see [Move a Scan to the Trash Folder (Classic Interface)](#).

You can delete custom scan folders only. You cannot delete the default scan folders that Tenable.io provides (*All Scans*, *My Scans*, and Trash).

**To create a folder:**

1. In the top navigation bar, click **Scans**.
   
   The *My Scans* page appears.

2. In the upper-right corner, click the **New Folder** button.
   
   The New Folder window appears.

3. In the **Name** box, type a name for the folder.

4. Click the **Create** button.
   
   The new folder appears in the left navigation bar.

**To move a scan to a folder:**
1. In the top navigation bar, click **Scans**. 
   The **My Scans** page appears.

2. If the scan you want to move is not in the **My Scans** folder, in the left navigation bar, click the folder that contains the scan you want to move.

3. In the scans table, select the check box next to the scan you want to configure.
   In the upper-right corner, the **More** button appears.

4. Click **More**.

5. Click **Move To**.

6. Click the folder where you want to move the scan.
   Tenable.io moves the scan to the folder you selected.

**To rename a folder:**

1. In the top navigation bar, click **Scans**.
   The **My Scans** page appears.

2. In the left navigation bar, click the **›** button next to the folder that you want to rename.

3. Click **Rename**.
   The **Rename Folder** window appears.

4. In the **Name** box, type a new name.

5. Click **Save**.
   The new name of the folder appears in the left navigation bar.

**To delete a folder:**

1. In the top navigation bar, click **Scans**.
   The **My Scans** page appears.

2. In the left navigation bar, click the **›** button next to the folder that you want to delete.

3. Click **Delete**.
The **Delete Folder** window appears.

4. Click **Delete**.

Tenable.io deletes the folder. If the folder contained scans, Tenable.io moves those scans to the **Trash** folder.
View Results for an Individual Scan (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can View

You can view scan results for scans you own or that the scan owners have shared with you.

Consider the following when viewing scan results:

- You can view results for an individual scan based on the permissions configured for the scan. However, when you view aggregated scan results in dashboards, including the **Vulnerabilities** and **Assets** workbenches, your access is based on the **access groups** you belong to.

- Tenable.io categorizes as "archived" any individual scan results that are older than 60 days. For scan results that are younger than 60 days, you can view and **export** the results in Tenable.io. For archived scan results, you can export the results, but cannot view them in Tenable.io. This limitation applies to both imported scan results and scan results that Tenable.io collects directly from scanners.

- When you view results from the last scan run, Tenable.io categorizes the scan as "read." You can also manually **change** the read status.

To view results for an individual scan:

1. In the top navigation bar, click **Scans**.
   - The **My Scans** page appears.

2. (Optional) In the left navigation bar, click a different folder.

3. In the scans table, click the name of the scan for which you want to view results.
   - The results page for that scan appears. The active tab on this page depends on the status of the scan.
In the right corner of the page, the **Scan Details** fields contain information about the latest scan run. This information includes:

- The date and time that the run started.
- The date and time the run ended.
- The status of the scan when the run ended.

**Note:** The **Elapsed** time includes the time Tenable.io Web Application Scanning takes to run the scan and process the results, as well as any time the scan spent in the pending scans queue.

The **Elapsed** value differs from the **Overall Max Scan Time** you configured when you created the scan, which includes only the scan run time.

4. Click the appropriate tab to view additional details:

   - [View Asset Details for an Individual Scan (Classic Interface)]
   - [View Vulnerability Details for an Individual Scan (Classic Interface)]
   - [View Audit Details for an Individual Scan (Classic Interface)]
   - [View Scan History Details (Classic Interface)]
   - [View Scan Notes (Classic Interface)]

**Note:** You can also [export](#) individual scan results from this page.
Change the Scan Read Status (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can View

When you view scans in the scans table, a scan appears in bold if you have not yet viewed (read) the results of the latest run of the scan.

If you view the scan results, Tenable.io categorizes the scan as "read" and removes the bold formatting from the scan in the scans table.

You can also use this procedure to manually change the scan read status.

To change the scan read status:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. If the scan you want to move is not in the **My Scans** folder, in the left navigation bar, click the folder that contains the scan you want to move.

3. In the scans table, select the check box next to each scan where you want to change the read status.

   The **More** button appears in the table header.

4. Click **More**.

   A drop-down list of options appears.

5. Click **Mark as Read** or **Mark as Unread**, as appropriate.

   Tenable.io changes the read status for the scan.
View Asset Details for an Individual Scan (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can View

The **Assets** tab appears on every scan results page, regardless of the scan status. If you configure a scan, but have not yet run it, the **Assets** tab is present but empty.

**Note:** You can view asset details for individual scan results that are younger than 60 days. For scan results older than 60 days, you can only export the results.

To view asset details for an individual scan:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the scans table, click the name of the scan for which you want to view scan results.
   
   The scan results page appears. The active tab on this page depends on the status of the scan.

3. Click the **Assets** tab.

**Note:** This tab does not appear if the scan results are older than 60 days.
The **Assets** tab appears.

On this page, you can view:
• The following charts:

<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerabilities</strong></td>
<td>The <strong>Vulnerabilities</strong> chart identifies vulnerabilities found by the scan, broken down by severity level. The severity levels are represented as percentages of the total number of vulnerabilities found. You can click specific sections of the chart to display the percentage for a specific severity level.</td>
</tr>
<tr>
<td><strong>Operating Systems</strong></td>
<td>The <strong>Operating Systems</strong> chart lists operating systems identified by the scan. Individual operating systems are represented as percentages of the total number of operating systems found. You can click specific sections of the chart to display the percentage for a specific operating system.</td>
</tr>
<tr>
<td><strong>Device Types</strong></td>
<td>The <strong>Device Types</strong> chart lists the different devices and platforms identified by the scan. Individual device types are represented as percentages of the total number of device types found. You can click specific sections of the chart to display the percentage for a specific device type.</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>The <strong>Authentication</strong> chart lists the authentication methods used during the scan. Individual authentication types are represented as percentages of the total number of types found. You can click specific sections of the chart to display the percentage for a specific authentication type.</td>
</tr>
</tbody>
</table>

• A table that lists in rows the target assets that were scanned and the vulnerabilities (if any) that were identified. Click an individual row to view more information about the vulnerabilities identified for that asset.
View Vulnerability Details for an Individual Scan (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can View

**Note:** You can view vulnerability details for individual scan results that are younger than 60 days. For scan results older than 60 days, you can only export the results.

To view vulnerability details for an individual scan:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the scans table, click the name of the scan for which you want to view scan results.
   
   The scan results page appears. The active tab on this page depends on the status of the scan.

3. Click the **Vulnerabilities** tab.

   **Note:** This tab does not appear if the scan run date is more than 60 days ago.
The **Vulnerability Details** page appears.

On this page you can view:

- **Current Vulnerabilities** widgets, which display the number of vulnerabilities identified the last time the scan completed, organized by severity level. Click on a box to view the specific vulnerabilities.

- The **Vulnerabilities** section, which includes the following charts:

<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploit Available</td>
<td>The <strong>Exploit Available</strong> chart displays the number of publicly available exploits target vulnerabilities detected on your assets.</td>
</tr>
<tr>
<td>Published Over 30 Days Ago</td>
<td>The <strong>Published Over 30 Days Ago</strong> chart displays the number of vulnerabilities detected on your assets that were published over 30 days ago.</td>
</tr>
<tr>
<td>Discovered Using Credentials</td>
<td>The <strong>Discovered Using Credentials</strong> chart displays the number of vulnerabilities detected on your assets that were discovered using system credentials.</td>
</tr>
</tbody>
</table>
### Chart Description

<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dentials</td>
<td>credentials.</td>
</tr>
<tr>
<td>Published Solutions Available</td>
<td>The <strong>Published Solutions Available</strong> chart displays the number of vulnerabilities detected on your assets that have remediation instructions available.</td>
</tr>
</tbody>
</table>

- A table of vulnerabilities detected during the scan. Each row represents a specific vulnerability, and includes the severity level, the **Name**, the **Family**, and the **Count**, or number of times the vulnerability was identified. The table is organized first by the level of severity of the vulnerability, and then in order of the number of times a vulnerability was detected. Click an individual row to view vulnerability information.
To view vulnerability information:

1. In the top navigation bar, click **Scans**. The **My Scans** page appears.

2. In the scans table, click the name of the scan for which you want to view scan results. The scan results page appears. The active tab on this page depends on the status of the scan.

3. Click the **Vulnerabilities** tab.

   **Note:** This tab does not appear if the scan run date is more than 60 days ago.

   The **Vulnerability Details** page appears.

4. Click the row of the vulnerability for which you wish to view more information. The **Vulnerability Information** page appears.
5. On this page, you can view:

- **A Description** of the vulnerability
- **Plugin Details** (including **Severity**, **ID**, **Type**, and **Family**)
- **Discovery details** (including **First Seen**, **Last Seen**, and **Age**)
- **Risk Information** (including **Risk Factor**, **Base Score**, and **Vector**)
- **A Solution** for the vulnerability
- **URLs** to the locations at which the vulnerabilities were found

If the vulnerability is a result of a Web Application Scan (WAS) and your browser is Google Chrome, the **View in App** button appears.

If you have the WAS Chrome Extension installed, Tenable.io opens the location at which the vulnerability was found and highlights the vulnerability on the page. If you do not have the WAS Chrome extension installed, Tenable.io opens the Google Chrome Store. For more information, see the [WAS Chrome Extension](#) documentation.
View Audit Details for an Individual Scan (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can View

**Note:** The Audits tab only appears on the Scan Results page if the scan is an audit scan.

**Note:** You can view audit details for individual scan results that are younger than 60 days. For scan results older than 60 days, you can only export the results.

To view audit details for an individual scan:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the scans table, click the name of the scan for which you want to view audit results.
   
   The results page for that scan appears. The active tab on this page depends on the status of the scan.

3. Click the **Audits** tab.
   
   **Note:** This tab does not appear if the scan run date is more than 60 days ago.

The **Audit Details** page appears.
On this page you can view:

- **Current Checks** widgets, which display the number of audit checks identified the last time the scan completed, organized by severity level. Click on a box to view the specific audit.

- A table of audits detected during the scan. Each row represents a specific audit, and includes the **Name**, the **Family**, and the **Count**, or number of times the audit was identified. The table is organized first by the level of severity of the audit, and then in order of the number of times an audit was detected. Click an individual row to view audit information.
To view audit information:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the scans table, click the name of the scan for which you want to view audit results.
   
   The results page for that scan appears. The active tab on this page depends on the status of the scan.

3. Click the **Audits** tab.

   **Note:** This tab does not appear if the scan run date is more than 60 days ago.

   The **Audit Details** page appears.

4. Click the audit where you want to view more information.

   The **Audit Information** page appears.
5. On this page, you can view:

- A **Description** of the audit
- **Reference Information** for the audit
- A **Solution** for the audit
**View Scan History Details (Classic Interface)**

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can View

Scan history includes the scan details for individual scan runs.

**Note:** Scan history is unavailable for imported scans.

To view scan history details:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the scans table, click the scan for which you want to view the scan history.
   
   The scan results page appears. The active tab on this page depends on the status of the scan.

3. Click the **History** tab.
   
   The **History** tab for the scan appears. On this tab, you can view a list of each time the scan has run.
4. In the scan history table, select a specific run:
   - For the latest scan run, click the row labeled **Current**.
   - For an earlier scan run, click any other row in the table.

   The **Scan Details** fields in the right corner of the page update to display information about the selected scan run.

5. Do one of the following:
   - Click the **Vulnerabilities** tab to view vulnerabilities identified during the selected scan run.
   - Click the **Assets** tab to view assets identified during the selected scan run.
   - Click the **Audits** tab to view audit details for the selected scan run.
   - Click the **Notes** tab to view problems encountered during the selected scan run.

**Note:** These tabs are only present if the scan results are younger than 60 days. For scan results older than 60 days, you can only export the results.
View Scan Notes (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can View

On the scan results page, the **Notes** tab appears only when Tenable.io encounters problems while running the scan.

**Note:** You can view notes for an individual scan run as long as the run date is less than 60 days ago. For scan results older than 60 days, you can only export the results.

To view scan notes:

1. In the top navigation bar, click **Scans**.

   The **My Scans** page appears.

2. In the scans table, click the scan where you want to view the scan notes.

   The scan results page appears. If Tenable.io encountered problems while running the latest scan, the **Notes** tab is active.

   **Note:** This tab does not appear if the scan run date is more than 60 days ago.

   The **Notes** page appears.

3. Review the scan notes to determine how to resolve the scan problem.

   For example, if an **Invalid Target** note is present, check the target parameters in the scan configuration.
Export Scan Results (Classic Interface)

**Video:** Export a Scan from Tenable.io

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can View

You can export both imported scan results and results that Tenable.io collects directly from scanners.

Tenable.io retains individual scan results until the results are 15 months old.

**Note:** For archived scan results (that is, results older than 60 days), the export format is limited to .nessus and .csv files.

To export results for an individual scan:

1. In the top navigation bar, click **Scans**.

   The **My Scans** page appears.

2. (Optional) In the left navigation bar, click a different folder.

   **Note:** If your Tenable.io Web Application Scanning license expires, Tenable.io removes all your web application scans from the scans table.

3. In the scans table, click the scan you want to export.

   The results page for that scan appears. By default, this page displays the most recent scan results. The active tab on this page depends on the status of the scan.

4. (Optional) **Select** the historical scan results you want to export.

5. In the upper-right corner of the page, click **Export**.

   A drop-down list of formats appears.
6. Select an export format:

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
<th>Supported for Archived Scan Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nessus</td>
<td>A <code>.nessus</code> file in XML format that contains the list of targets, policies defined by the user, and scan results. Password credentials are stripped so they are not exported as plain text in the XML. If you import a <code>.nessus</code> file as a policy, you must re-apply your passwords to any credentials.</td>
<td>Yes</td>
</tr>
<tr>
<td>PDF</td>
<td>An Adobe <code>.pdf</code> file.</td>
<td>No</td>
</tr>
<tr>
<td>HTML</td>
<td>A web-based <code>.html</code> file.</td>
<td>No</td>
</tr>
<tr>
<td>CSV</td>
<td>A comma-separated value (.csv) text file.</td>
<td>Yes</td>
</tr>
<tr>
<td>DB (WAS only)</td>
<td>A SQL database export of all scan data (including scan notes and attachments). The scan results are encrypted and can only be viewed in a Tenable.io or Nessus application. You can export scan results as a database to send to Tenable Support for troubleshooting or to import in another Tenable.io or Nessus account. When you select this option, a window with a <strong>Password</strong> box appears. Type a password to use for the encryption.</td>
<td>No</td>
</tr>
</tbody>
</table>

**Note:** Passwords must be at least 1 character.

7. Continue as appropriate:
• For the **Nessus** and **CSV** formats, no additional action is needed.

  Depending on your browser settings, Tenable.io may automatically download the export file to your computer.

• For the **PDF** or **HTML** formats:
  
  a. In the Select a report format: **Executive Summary** or **Custom**.
  
  b. If you select **Custom**:
    
    • Retain the default **Data** setting (**Vulnerabilities** selected).
    
    • Select either **Assets** or **Plugin** from the **Group By** list, depending on how you want to group the scan results in the export file.
  
  c. Click **Export**.

  Tenable.io generates the export file. Depending on your browser settings, Tenable.io may automatically download the export file to your computer.
Policies (Classic Interface)

A policy is a set of predefined configuration options related to performing a scan. After you create a policy, you can select it as a template when you create a scan.

**Note:** For information about default policy templates and settings, see the following topics:
- Templates
- Settings

The following are characteristics of policies:

- Parameters that control technical aspects of the scan such as timeouts, number of hosts, type of port scanner, and more.
- Credentials for local scans (e.g., Windows, SSH), authenticated Oracle database scans, HTTP, FTP, POP, IMAP, or Kerberos based authentication.
- Granular family or plugin-based scan specifications.
- Database compliance policy checks, report verbosity, service detection scan settings, Unix compliance checks, and more.
- Offline configuration audits for network devices, allowing safe checking of network devices without needing to scan the device directly.
Windows malware scans which compare the MD5 checksums of files, both known good and malicious files.

For more information on Policies, see the following topics:

- [Create a Policy](#)
- [Copy a Policy](#)
- [Import a Policy](#)
- [Export a Policy](#)
- [Set Permissions for a Policy](#)
- [Delete a Policy](#)
Create a Policy (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Standard, Scan Manager, or Administrator

When you create a policy, Tenable.io assigns you owner permissions for the policy. You can share the policy by assigning policy permissions to other users, but only you can delete the policy.

To create a scan policy:

1. In the top navigation bar, click **Scans**.
   The **My Scans** page appears.
2. In the left navigation bar, click **Policies**.
   The **Policies** page appears.
3. In the upper-right corner, click the **New Policy** button.
   The **New Policy** page appears.
4. Select a **policy template**.
5. In the **Settings** tab, manage the **policy settings**.
6. (Optional) In the **Credentials** tab, add **credentials** to the policy.
   **Note:** Any credentials added to a scan (managed or scan-specific) override policy-specific credentials. Tenable recommends adding managed credentials to scans, instead of adding credentials to policies.
7. (Optional) In the **Compliance** tab, specify which **platforms** you want to audit for compliance. Tenable, Inc. provides best practice audits for each platform. Additionally, you can upload a custom audit file.
8. (Optional; Advanced Network Scan only) In the **Plugins** tab, select security checks by **plugin**.
9. Click **Save**.
   Tenable.io creates the policy and assigns you owner permissions for the policy.
Copy a Policy (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Standard, Scan Manager, or Administrator

**Required Policy Permissions:** Can Configure

When you copy a policy, Tenable.io assigns you owner permissions for the copy. You can share the copy by assigning [policy permissions](https://tenable.com) to other users, but only you can [delete](https://tenable.com) the copied policy.

To copy a scan policy:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Policies**.

   The **Policies** page appears.

3. In the policies table, select the check box next to the policy you want to copy.

4. In the top navigation bar, click **More**.

5. Click **Copy**.

   Tenable.io creates a copy of the policy with *Copy of* prepended to the name and assigns you owner permissions for the copy. The copy appears in the policies table.
Import a Policy (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Standard, Scan Manager, or Administrator

When you import a policy, Tenable.io assigns you owner permissions for the policy. You can share the policy by assigning *policy permissions* to other users, but only you can *delete* the policy.

To import a scan policy:

1. In the top navigation bar, click **Scans**.
   
The **My Scans** page appears.

2. In the left navigation bar, click **Policies**.
   
The **Policies** page appears.

3. In the upper-right corner, click the **Import** button.
   
The file explorer for your operating system appears.

4. Select a .nessus policy file to import.
   
   Tenable.io imports the policy configuration and adds the policy to the table on the **Policies** page.
Export a Policy (Classic Interface)

Required Tenable.io Vulnerability Management User Role: Standard, Scan Manager, or Administrator

Required Policy Permissions: Can Configure

Note: Tenable.io does not export passwords or .audit files contained in a policy.

To export a scan policy:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Policies**.
   
   The **Policies** page appears.

3. In the table of policies, click the **button next to the policy you want to export.

   The policy downloads automatically in .nessus format.
Change Policy Ownership (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

**Required Scan Permissions:** Owner

To change the ownership of a policy:

1. In the top navigation bar, click **Scans**.
   
The *My Scans* page appears.

2. In the left navigation bar, click **Policies**.
   
The policies table appears.

3. In the policies table, click the row of the policy you want to modify.
   
The *Configuration* table appears. By default, the *Settings* tab is selected.

4. In the **Basic** settings section, click **Permissions**.
   
The *User Sharing* settings appear.

5. In the **User Sharing** section, in the **Owner** drop-down box, select a new user to assign ownership.

6. Click **Save**.

  Tenable assigns ownership to the selected user.
Set Policy Permissions (Classic Interface)

Required Tenable.io Vulnerability Management User Role: Standard, Scan Manager, or Administrator

Required Policy Permissions: Can Configure

To set policy permissions:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Policies**.

3. In the policies table, click the policy you want to configure.
   
   The policy page appears.

4. In the **Settings** tab, under **Basic**, click **Permissions**.
   
   The **User Sharing** settings appear.

5. Modify the [permissions settings](https://tenable.com).

6. Click **Save**.
   
   Tenable.io updates the policy permissions.
Delete a Policy (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Standard, Scan Manager, or Administrator

**Required Policy Permissions:** Owner

If you delete a user-defined policy, Tenable.io deletes it from all user accounts.

**Before you begin:**

- [Delete](#) any scans that use the policy you want to delete. You cannot delete a policy if a scan is using the policy.

**To delete a policy:**

1. In the top navigation bar, click **Scans**.
   
The **My Scans** page appears.

2. In the left navigation bar, click **Policies**.
   
The **Policies** page appears.

3. In the list of policies, click the [ ] button next to the policy you want to delete.
   
The **Delete Policy** window appears, prompting you to confirm the deletion.

4. Click the **Delete** button.
   
   Tenable.io deletes the policy.

**To delete multiple policies:**

1. In the top navigation bar, click **Scans**.
   
The **My Scans** page appears.

2. In the left navigation bar, click **Policies**.
   
The **Policies** page appears.

3. In the list of policies, select the check boxes next to the policies you want to delete.
4. In the upper-right corner, click the **Delete** button.

   The **Delete Policies** window appears, confirming your selection to delete the policies.

5. Click the **Delete** button.

   The policies are deleted.
Scanners (Classic Interface)

**Note:** This section describes the classic Tenable.io interface. For an introduction to the new interface, see Sensors.

By default, Tenable.io is configured with a regional, specific cloud scanner. In addition to using the default cloud scanner, users can also link Nessus instances, NNM instances, and Nessus Agents to Tenable.io. These linked sensors are called "remote scanners." For more information, see [Link a Scanner](#).

Once linked to Tenable.io, you can add the remote scanners to **Scanner Groups**. You can also manage and select remote scanners when configuring scans.

Scanners can be assigned to custom networks. For more information, see [Networks](#).

You must install a Nessus scanner or NNM instance on a host before you can [link the scanner to Tenable.io](#).

The **Linked Scanners** page displays scanner names, types, and permissions.

### Cloud Scanners

By default, Tenable.io is configured with region-specific Cloud Scanners. You can select these scanners when you create and launch scans.

The Tenable.io interface displays the following Cloud Scanners:

- **US Cloud Scanner**: A group of scanners from one US-EAST range (Ohio or Virginia) and the US-WEST range.

- **US East Cloud Scanners**: A group of scanners from either the Ohio or Virginia US-EAST range.

- **US West Cloud Scanners**: A group of scanners from the US-WEST range.

- **AP Singapore Cloud Scanners**: A group of scanners from the Singapore AP-SOUTHEAST range.

- **AP Sydney Cloud Scanners**: A group of scanners from the Sydney AP-SOUTHEAST range.

- **AP Tokyo Cloud Scanners**: A group of scanners from the AP-NORTHEAST-1 range.
• **CA Central Cloud Scanners**: A group of scanners from the CA-CENTRAL-1 range.

• **EU Frankfurt Cloud Scanners**: A group of scanners from the EU-CENTRAL range.

• **UK Cloud Scanners**: A group of scanners from the EU-WEST-2 (London) range.

• **APAC Cloud Scanners**: A group of scanners from the following AWS ranges:
  - AP-SOUTHEAST-1 (Singapore)
  - AP-SOUTHEAST-2 (Sydney)
  - AP-NORTHEAST-1 (Tokyo)

• **EMEA Cloud Scanners**: A group of scanners from the following AWS ranges:
  - Amazon EU-CENTRAL (Frankfurt)
  - Amazon EU-WEST (London)

The following table identifies each Tenable.io Scanner and, for whitelisting purposes, its IP address range. These IP ranges are exclusive to Tenable, Inc.

<table>
<thead>
<tr>
<th>Sensor</th>
<th>IP Range</th>
<th>IPv6 Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon CA-CENTRAL-1 (Canada)</td>
<td>35.182.14.64/26</td>
<td>2600:1f11:622:3000::/56</td>
</tr>
<tr>
<td></td>
<td>3.98.92.0/25</td>
<td></td>
</tr>
<tr>
<td>Amazon US-EAST (Ohio or Vir-</td>
<td>13.59.252.0/25</td>
<td>2600:1f16:8ca:e900::/56</td>
</tr>
<tr>
<td>ginia)</td>
<td>54.175.125.192/26</td>
<td></td>
</tr>
<tr>
<td></td>
<td>34.201.223.128/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.132.217.0/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>18.116.198.0/24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>44.192.244.0/24</td>
<td></td>
</tr>
<tr>
<td>Amazon US-WEST (California or</td>
<td>54.219.188.128/26</td>
<td>2600:1f1c:13e:9e00::/56</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note**: If you use cloud connectors, Tenable recommends allowing the IP addresses for the region in which the Tenable.io site resides.
<table>
<thead>
<tr>
<th>Sensor</th>
<th>IP Range</th>
<th>IPv6 Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oregon)</td>
<td>13.56.21.128/25</td>
<td>2600:1f14:141:7b00::/56</td>
</tr>
<tr>
<td></td>
<td>34.223.64.0/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>44.242.181.128/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.101.175.0/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>35.82.51.128/25</td>
<td></td>
</tr>
<tr>
<td>Amazon EU-CENTRAL (Frankfurt)</td>
<td>54.93.254.128/26</td>
<td>2a05:d014:532:b00::/56</td>
</tr>
<tr>
<td></td>
<td>18.194.95.64/26</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.124.123.128/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.67.7.128/25</td>
<td></td>
</tr>
<tr>
<td>Amazon EU-WEST (London)</td>
<td>35.177.219.0/26</td>
<td>2a05:d01c:da5:e800::/56</td>
</tr>
<tr>
<td></td>
<td>3.9.159.128/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>18.168.180.128/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>18.168.224.128/25</td>
<td></td>
</tr>
<tr>
<td>Amazon AP-SOUTHEAST (Singapore)</td>
<td>54.255.254.0/26</td>
<td>2406:da18:844:7100::/56</td>
</tr>
<tr>
<td></td>
<td>18.139.204.0/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>13.213.79.0/24</td>
<td></td>
</tr>
<tr>
<td>Amazon AP-SOUTHEAST (Sydney)</td>
<td>13.210.1.64/26</td>
<td>2406:da1c:20f:2f00::/56</td>
</tr>
<tr>
<td></td>
<td>3.106.118.128/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.26.100.0/24</td>
<td></td>
</tr>
<tr>
<td>Amazon AP-NORTHWEST-1 (Tokyo)</td>
<td>13.115.104.128/25</td>
<td>2406:da14:e76:5b00::/56</td>
</tr>
<tr>
<td></td>
<td>35.73.219.128/25</td>
<td></td>
</tr>
<tr>
<td>Amazon AP-SOUTH (Mumbai)</td>
<td>3.108.37.0/24</td>
<td>2600:1f1e:9a:ba00::/56</td>
</tr>
</tbody>
</table>
Scan ranges may also be grouped into the following categories:

<table>
<thead>
<tr>
<th>Sensor</th>
<th>IP Range</th>
<th>IPv6 Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon SA-EAST (São Paulo)</td>
<td>15.228.125.0/24</td>
<td>2406:da1a:5b2:8500::/56</td>
</tr>
<tr>
<td>APAC Cloud Scanners</td>
<td>54.255.254.0/26</td>
<td>2406:da18:844:7100::/56</td>
</tr>
<tr>
<td></td>
<td>18.139.204.0/25</td>
<td>2406:da1c:da5:e800::/56</td>
</tr>
<tr>
<td></td>
<td>13.210.1.64/26</td>
<td>2406:da14:e76:5b00::/56</td>
</tr>
<tr>
<td></td>
<td>3.106.118.128/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.26.100.0/24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>13.115.104.128/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>35.73.219.128/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.108.37.0/24</td>
<td></td>
</tr>
<tr>
<td>EMEA Cloud Scanners</td>
<td>54.93.254.128/26</td>
<td>2a05:d014:532:b00::/56</td>
</tr>
<tr>
<td></td>
<td>18.194.95.64/26</td>
<td>2a05:d01c:da5:e800::/56</td>
</tr>
<tr>
<td></td>
<td>3.124.123.128/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.67.7.128/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>35.177.219.0/26</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.159.128/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>18.168.180.128/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>18.168.224.128/25</td>
<td></td>
</tr>
</tbody>
</table>

**Tip:** In addition to the above listed IP address ranges, the following can be used for whitelisting cloud.tenable.com for internal scanner or agent communications:

- 162.159.129.83/32
- 162.159.130.83/32
Linked Scanners

In addition to using Tenable.io scanners, you can also link Nessus and NNM scanners to Tenable.io.

**Note:** You can assign linked sensors to custom networks. For more information, see [Networks](#).

The *Linked Scanners* page displays the Tenable.io *Linking Key*, identifies scanners by scanner type (Nessus or NNM) and indicates if the scanners have *Shared permissions*.

Use the *Linking Key* when installing and connecting Nessus Manager, Nessus Agent, or NNM scanners.

- **Manager Host**: cloud.tenable.com
- **Manager Port**: 443

From the *Linked Scanner* page, you can:
• Open a linked scanner to view or modify its settings.
• **Enable or disable** a linked scanner.
• **Remove** a linked scanner.
• **Download logs** for a linked scanner.
Link a Scanner (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

This procedure describes how to link a Nessus scanner or NNM to Tenable.io. Once linked, a scanner can be managed locally and selected when configuring Tenable.io scans.

**Video:** [Link a Scanner to Tenable.io](#)

To link a scanner:

1. In Tenable.io, click **Scans > Scanners**.
   
   The **Scanners** section appears.

2. In the **Linked Scanners** subsection, copy the **Linking Key**.

3. Access the Nessus scanner or NNM instance.

4. Link the Nessus scanner or NNM instance to Tenable.io.

For more information about the linking options, see the [Nessus User Guide](#), [NNM User Guide](#), or [Tenable Core + Tenable.io Web Application Scanning User Guide](#).
Modify Scanner Permissions (Classic Interface)

Required Tenable.io Vulnerability Management User Role: Scan Manager or Administrator

You can set the following Tenable.io user permissions levels in your scanner configuration:

- **No Access** - The user or group cannot use the scanner in scan configurations or modify the scanner configuration.

- **Can Use** - The user or group can use the scanner in scan configurations, but cannot modify the scanner configuration.

- **Can Manage** - The user or group can use the scanner in scan configurations and modify the scanner configuration.

To modify scanner permissions:

1. In the top navigation bar, click **Scans**.

   The **My Scans** page appears.

2. In the left navigation bar, click **Scanners**.

   The **Scanners** page appears.

3. In the scanners table, click the scanner you want to modify.

   The **Edit Scanner** page appears.

4. Click the **Permissions** tab.

   On this tab, you can add users or groups and adjust permissions.
Enable or Disable a Scanner (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

To enable or disable a scanner:

**To enable a scanner:**

1. In the top navigation bar, click Scans.
   
   The My Scans page appears.

2. In the left navigation bar, click Scanners.
   
   The Scanners page appears.

3. In the scanners table, click the button next to the scanner you want to enable.
   
   Tenable.io enables the scanner.

**To disable a scanner:**

1. In the top navigation bar, click Scans.
   
   The My Scans page appears.

2. In the left navigation bar, click Scanners.
   
   The Scanners page appears.

3. In the scanners table, click the button next to the scanner you want to disable.
   
   Tenable.io disables the scanner.
Remove a Scanner (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

To remove a scanner:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Scanners**.
   
   The **Scanners** page appears.

3. In the scanners table, click the **X** button next to the scanner you want to remove.

4. Click **Remove** to confirm the removal.
   
   Tenable.io remove the scanner from the list.
Download Managed Scanner Logs (Classic Interface)

Required Tenable.io Vulnerability Management User Role: Scan Manager or Administrator

In Tenable.io, you can request and download a log file containing logs and system configuration data from any of your managed scanners and Nessus Agents. This information can help you troubleshoot system problems, and also provides an easy way to gather data to submit to Tenable Support.

You can store a maximum of five log files from each managed scanner in Tenable.io. Once the limit is reached, you must remove an old log file to download a new one.

Note: You can only request logs from Nessus scanners running 8.1 and later.

To download logs from a managed scanner:

1. In the top navigation bar, click Scans.
   - The My Scans page appears.

2. In the left navigation bar, click Scanners.
   - The Scanners page appears.

3. In the linked scanners table, click the scanner for which you want to download logs.
   - The detail page for that scanner appears.

4. Click the Logs tab.

5. In the upper-right corner, click Request Logs.
   - Note: If you have reached the maximum of five log files, the Request Logs button is disabled. Remove an existing log before downloading a new one.

   Tenable.io requests the logs from the managed scanner the next time it checks in, which may take several minutes. You can view the status of the request in the user interface until the download is complete.

6. To download the log file, click the file name.
   - Your system downloads the log file.
To remove an existing log:

- In the row of the log you want to remove, click the trash can button.

To cancel a pending or failed log download:

- In the row of the pending or failed log download that you want to cancel, click the stop button.
Scanner Settings (Classic Interface)

Scanner settings control how frequently linked scanners report information to Tenable.io.

To modify the settings, see Modify Scanner Settings (Classic Interface).

<table>
<thead>
<tr>
<th>Scanner Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NNM scanner</td>
<td></td>
</tr>
<tr>
<td>Report Frequency</td>
<td>Specifies the frequency, in minutes, at which NNM reports information to Tenable.io.</td>
</tr>
<tr>
<td>Automatic Updates</td>
<td>(NNM 5.6.1 and later only) Specifies which components, if any, you want NNM to automatically update. All components includes web server, HTML client, plugins, and engine.</td>
</tr>
<tr>
<td>AWS scanner</td>
<td></td>
</tr>
<tr>
<td>Updates instances every X minutes</td>
<td>Specifies the frequency (in minutes) at which the AWS scanner reports information to Tenable.io about the instances it has access to.</td>
</tr>
</tbody>
</table>
Modify Scanner Settings (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

You can modify the settings of a linked scanner to control how frequently the scanner sends information to Tenable.io.

To modify scanner settings:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Scanners**.
   
   The **Scanners** page appears.

3. In the scanners table, click the scanner you want to modify.
   
   The **Edit Scanner** page appears.

4. Click the **Settings** tab.

5. Modify the **settings** you want to edit for your scanner.

6. Click **Save**.
Scanner Groups (Classic Interface)

In Tenable.io, you can link a variety of scanners to your account. You can also use scanner groups to organize and manage the scanners linked to your account. For example, you can add all scanners related to a specific geographical location to a group (for example, a group called East Coast Scanners). You can add a scanner to one or more scanner groups. Then, when you create a scan, you can select the scanner group to use to launch the scan.

![Scanner Groups](image)

When you configure a **Scanner Group** for scan operations, Tenable.io determines the scanner(s) to use based on the following criteria:

- The scanner(s) are active and have communicated to Tenable.io within the last 5 minutes.
- The scanner(s) running are running the lowest number of active scans and are scanning the lowest number of hosts.

**Note:** If a remote scanner is part of a **Scanner Group** and is unlinked during its operations, the scan’s operations complete, but Tenable.io does not include the unlinked scanner for future use.

For more information on **Scanner Groups**, see the following topics:

- [Create a Scanner Group (Classic Interface)]
- [Edit a Scanner Group (Classic Interface)]
- [Delete a Scanner Group (Classic Interface)]
Create a Scanner Group (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

To create a scanner group:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Scanners**.

   The **Scanners** page appears.

3. Click the **Scanner Groups** tab.

4. In the upper-right corner, click the **New Group** button.

5. In the **New Scanner Group** box, type a name for the group.

6. Click the **Add** button.

   The **Edit Scanner Group** page appears, where you can manage scanners, scans, scanner group settings, and permissions.
Edit a Scanner Group (Classic Interface)

Required Tenable.io Vulnerability Management User Role: Scan Manager or Administrator

To edit a scanner group:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Scanners**.
   
   The **Scanners** page appears.

3. Click the **Scanner Groups** tab.

4. In the list of scanner groups, click the scanner group you want to modify.
   
   The **Edit Scanner Group** page appears, where you can manage scanners, scans, scanner group settings, and permissions.
Delete a Scanner Group (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

To delete one or more scanner groups:

**To delete one scanner group:**

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Scanners**.
   
   The **Scanners** page appears.

3. Click the **Scanner Groups** tab.

4. In the list of scanner groups, click the ✗ button next to the scanner group you want to delete.
   
   The **Delete Group** window appears, confirming your selection to delete the group.

5. Click the **Delete** button.

   Tenable.io deletes the group.

**To delete multiple scanner groups:**

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Scanners**.
   
   The **Scanners** page appears.

3. Click the **Scanner Groups** tab.

4. In the list of scanner groups, select the check boxes next to the scanner groups you want to delete.

5. In the upper-right corner, click the **Delete** button.
   
   The **Delete Groups** window appears, prompting you to confirm the deletion.
6. Click the **Delete** button.

   Tenable.io deletes the groups you selected.
Networks (Classic Interface)

**Note:** You can only manage networks in the classic Tenable.io interface.

**Video:** Overlapping IP Support in Tenable.Tenable.io

In larger enterprises, you can reduce the time and cost of setting up and maintaining locations by deploying environments with the same internal IP addresses. To disambiguate between assets that have the same IP addresses across environments, use networks in Tenable.io.

If you deploy environments with the same internal IP addresses, create a network for each environment you have, and assign scanners and scanner groups to each network. When a scanner scans an asset, the associated network is added to the asset's details. You can filter assets by network or create dynamic tags based on a network. Recast rules and access groups do not support networks.

A scanner or scanner group can only belong to one network at a time.

There are two types of networks:

- **Default network** – The network to which a scanner or scanner group belongs unless you assign it to a custom network.
  
  You can view scanners in the default network, but you cannot add or remove scanners from the default network.

  If you remove a scanner or scanner group from a custom network, or if you delete a custom network, Tenable.io returns the scanner or scanner groups to the default network.

  Imported scans always belong to the default network.

- **Custom network** – A network you create. Add a custom network only if you want to scan targets in separate environments that contain overlapping IP ranges. If your scans do not involve separate environments with overlapping IP ranges, keep all scanners in the Default network.

For more information on networks, see the following topics:

- [Create a Network (Classic Interface)]
- [View or Edit a Network (Classic Interface)]
- Add a Scanner to a Network (Classic Interface)
- Remove a Scanner from a Network (Classic Interface)
- Move Assets to a Network (Classic Interface)
- Delete Assets from a Network (Classic Interface)
- Delete a Network (Classic Interface)
Create a Network (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Create a custom network only if you want to scan targets in separate environments that contain overlapping IP ranges. If your scans do not involve separate environments with overlapping IP ranges, keep all scanners in the **Default** network.

To create a new network:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.
2. In the left navigation bar, click **Scanners**.
   
   The **Scanners** page appears.
3. Click the **Networks** tab.
   
   The **Networks** page appears. This page contains a table listing the default network and all custom networks in your Tenable.io instance.
4. Click **New Network**.
   
   The **New Network** dialog box appears.
5. In the **Name** box, type a name for the network.
   
   The name can contain any alphanumeric and special characters except < and >.
6. (Optional) In the **Description** box, type a description for the network.
7. Click **Add**.
   
   The **New Network Created** confirmation box appears.
8. Do one of the following:

   Move assets to the network now:
   
   a. Click **Move Assets**.
      
      The **Move Assets to Network** dialog box appears.
b. From the **Source Network** drop-down box, select the network that contains the assets you want to move.

c. In the text box, type the IPv4 addresses of the assets you want to move, in the format of a comma-separated list, range, or subnet with CIDR notation.

d. Click **Search**.

   Tenable.io displays the number of assets that match your search.

e. Click **Move**.

   Tenable.io creates the network and moves the selected assets to the network.

**Move assets to the network later:**

a. Click **Cancel**.

   Tenable.io creates the network.

b. **Add scanners and scanner groups** to the network.

c. **Move assets to the network.**
Add a Scanner to a Network (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

A scanner or scanner group is part of the default network unless you add it to a custom network. A scanner or scanner group can only be part of one network at a time.

You can only add a scanner group to a custom network if all scanners in that group belong to either the default network or the same custom network. If you try to add a scanner group that contains a scanner already assigned to a different custom network, Tenable.io prevents you from adding the scanner group to the network until you resolve the conflict.

To add a scanner or scanner group to a network:

1. In the top navigation bar, click **Scans**.
   
The **My Scans** page appears.

2. In the left navigation bar, click **Scanners**.
   
The **Scanners** page appears.

3. Click the **Networks** tab.
   
The **Networks** page appears. This page contains a table listing the default network and all custom networks in your Tenable.io instance.

4. In the networks table, click the network where you want to add scanners.
   
The **Edit Network** page appears.

5. In the **Available Scanners** table, click the button next to the scanner or scanner group you want to add.

   Tenable.io determines whether there are any scanner group conflicts:

   - If no conflicts are present, Tenable.io adds the scanner or scanner group to the network and moves it to the **Member Scanners** table.
• If any conflicts are present, Tenable.io displays a message that lists which scanners you must remove from the scanner group to resolve the conflict. For more information about removing scanners from scanner groups, see Edit a Scanner Group.
Remove a Scanner from a Network (Classic Interface)

Required Tenable.io Vulnerability Management User Role: Scan Manager or Administrator

If you remove a scanner or a scanner group from a custom network, Tenable.io reassigns it to the default network.

Tip: If you want to delete a scanner group or remove a scanner from a scanner group, see Delete a Scanner Group (Classic Interface) and Remove a Scanner (Classic Interface).

To remove a scanner or scanner group from a custom network:

1. In the top navigation bar, click **Scans**.

   The **My Scans** page appears.

2. In the left navigation bar, click **Scanners**.

   The **Scanners** page appears.

3. Click the **Networks** tab.

   The **Networks** page appears. This page contains a table listing the default network and all custom networks in your Tenable.io instance.

4. In the **Member Scanners** table, click the ✗ button next to the scanner or scanner group you want to remove.

   Tenable.io moves the scanner or scanner group to the default network. The scanner or scanner group appears in the **Available Scanners** table.
View or Edit a Network (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

To view or edit the configuration of an existing network:

1. In the top navigation bar, click **Scans**.
   
The **My Scans** page appears.
2. In the left navigation bar, click **Scanners**.
   
The **Scanners** page appears.
3. Click the **Networks** tab.
   
The **Networks** page appears. This page contains a table listing the default network and all custom networks in your Tenable.io instance.
4. In the networks table, click the network you want to edit.
   
The **Edit Network** page appears.
5. In the **Manage Scanners** tab, you can do the following:

<table>
<thead>
<tr>
<th>Table</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Scanners</td>
<td>• View scanners and scanner groups currently assigned to the default network.</td>
</tr>
<tr>
<td></td>
<td>• Add a scanner or scanner group to the custom network you are currently editing by clicking the button in the row of the scanner or scanner group.</td>
</tr>
<tr>
<td>Member Scanners</td>
<td>• View scanners and scanner groups assigned to the custom network you are currently editing.</td>
</tr>
<tr>
<td></td>
<td>• Remove a scanner or scanner group from the network by clicking the button in the row of the scanner or scanner group.</td>
</tr>
</tbody>
</table>

6. In the **Settings** tab:
a. Edit the name and description of the network.
   The name can contain any alphanumeric and special characters except < and >.

b. Click **Save**.
Move Assets to a Network (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

When a scanner scans assets, the scanner automatically adds the network to which it belongs to scanned assets' identifying details. However, if you want to change the network assets are assigned to, you can also manually move assets to a network.

To move assets to a network:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Scanners**.

   The **Scanners** page appears.

3. Click the **Networks** tab.

   The **Networks** page appears. This page contains a table listing the default network and all custom networks in your Tenable.io instance.

4. In the table, click the : button next to the network to which you want to move assets.

   A drop-down box appears.

5. Click **Move Assets**.

   The **Move Assets to Network** dialog box appears.

6. From the **Source Network** drop-down box, select the network that contains the assets you want to move.

7. In the text box, type the IPv4 addresses of the assets you want to move, in the format of a comma-separated list, range, or subnet with CIDR notation.

8. Click **Search**.

   Tenable.io displays the number of assets that match your search.

**Tip:** To view the assets that match your search, click **View Results in a New Tab**.
9. Click **Move**.

Tenable.io moves the selected assets to the network.

**Note:** Tenable.io may take some time to move the assets, depending on the system load, the number of matching assets, and the number of vulnerabilities.
Delete Assets from a Network (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

You can delete assets by filtering for IP addresses on a network and deleting the assets that match the filter.

When you delete an asset, Tenable.io deletes the asset from the default view of the assets table, deletes vulnerability data associated with the asset, and stops matching scan results to the asset. To view deleted assets, see [View Deleted Assets](#).

**Tip:** If you want to remove an asset from a network but not delete the asset, see [Move Assets to a Network (Classic Interface)](#).

To delete assets from a network:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Scanners**.
   
   The **Scanners** page appears.

3. Click the **Networks** tab.
   
   The **Networks** page appears. This page contains a table listing the default network and all custom networks in your Tenable.io instance.

4. In the table, click the ⌂ button next to the network that contains the assets you want to delete.
   
   A drop-down box appears.

5. Click **Delete Assets**.
   
   The **Delete Assets from Network** dialog box appears.

6. In the text box, type the IPv4 addresses of the assets you want to delete, in the format of a comma-separated list, range, or subnet with CIDR notation.

7. Click **Search**.
Tenable.io displays the number of assets that match your search.

**Tip:** To view the assets that match your search, click **View Results in a New Tab**.

8. Click **Delete**.

Tenable.io deletes the selected assets.

**Note:** Tenable.io may take some time to delete the assets, depending on the system load, the number of matching assets, and the number of vulnerabilities.
Delete a Network (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Before you begin:

Before you delete a network, consider the following:

- Tenable.io re-assigns any scanners or scanner groups in the deleted network to the default network. If you want to delete the scanners or scanner groups, see [Remove a Scanner (Classic Interface)] and [Delete a Scanner Group (Classic Interface)].

- After you delete a network, assets that were in the deleted network still retain the network attribute. Consider moving assets to a different network before you delete the network. To move assets from a deleted network to another network, you must use the [API].

- Tenable.io retains any asset records for the deleted network until the assets age out of your licensed assets count. You can still filter for assets that use the deleted network.

- You cannot create a new network that has the same name as a deleted network.

To delete a network:

1. In the top navigation bar, click Scans.
   
   The My Scans page appears.

2. In the left navigation bar, click Scanners.

   The Scanners page appears.

3. Click the Networks tab.

   The Networks page appears. This page contains a table listing the default network and all custom networks in your Tenable.io instance.

4. In the networks table, click the ❌ button next to the network you want to delete.

   The Delete Network dialog box appears.

5. To confirm you want to delete the network, click Delete.

   Tenable.io deletes the network.
Agents (Classic Interface)

**Note:** This section describes the classic Tenable.io interface. For an introduction to the new interface, see [Agents](#).

Agents increase scan flexibility by making it easy to scan assets without needing ongoing host credentials or assets that are offline. Additionally, agents enable large-scale concurrent scanning with little network impact.

After you install **Nessus Agents** on a host, the Agent appears on the Tenable.io **Linked Agents** page.

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Last Scanned</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS Linux Agent</td>
<td>192.168.03.40</td>
<td>10/06/16</td>
</tr>
<tr>
<td>Windows NT Agent</td>
<td>192.168.3.93</td>
<td>09/10/14</td>
</tr>
<tr>
<td>Windows XP Agent</td>
<td>192.168.245.23</td>
<td>10/19/16</td>
</tr>
<tr>
<td>Windows XP/98/95 Agent</td>
<td>192.168.233.29/24</td>
<td>09/09/16</td>
</tr>
</tbody>
</table>

For more information, see the following topics:

- [Retrieve the Nessus Agent Linking Key (Classic Interface)](#)
- [Agent Settings (Classic Interface)](#)
- [Agent Status (Classic Interface)](#)
- [Filter Agents (Classic Interface)](#)
- [Export Agents (Classic Interface)](#)
• Unlink an Agent (Classic Interface)
• Download Linked Agent Logs (Classic Interface)
• Agent Groups (Classic Interface)
• Blackout Windows (Classic Interface)
Retrieve the Nessus Agent Linking Key (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Before you begin the Nessus Agent installation process, you must retrieve the Nessus Agent Linking Key from Tenable.io.

**Video:** Link an Agent to Tenable.io

To retrieve the linking key:

1. In the top navigation bar, click **Scans**.
   
The **My Scans** page appears.

2. In the left navigation bar, click **Agents**.
   
The **Agents** page appears.

3. In the **Linked Agents** tab, click the **setup instructions** link.
   
The **Agent Setup Instructions** dialog box appears.

4. Record the **host**, **port**, and **key** values.

<table>
<thead>
<tr>
<th>Option</th>
<th>Set To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link a Nessus Agent to Tenable.io</td>
<td></td>
</tr>
<tr>
<td>Host</td>
<td>cloud.tenable.com</td>
</tr>
<tr>
<td>Port</td>
<td>443</td>
</tr>
<tr>
<td>Key</td>
<td>The Linking Key specific to your instance of Tenable.io. For example:</td>
</tr>
<tr>
<td></td>
<td>2d38415603b5b59a4526e39640655c3288a00324097a08f7a93e5480940d1-</td>
</tr>
<tr>
<td></td>
<td>cae</td>
</tr>
</tbody>
</table>

5. Click **Close**.

What to do next:

- **Install Nessus Agents**
### Agent Settings (Classic Interface)

On your agent's manager, you can configure system-wide agent settings to specify agent and blackout window settings for all your linked agents. For more information on creating, modifying, and deleting blackout windows, see Blackout Windows.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inactive Agents</strong></td>
<td>Specifies the number of days an agent can be inactive before the manager unlinks the agent. After the specified number of days, the agent is unlinked, but the corresponding agent data is not removed from the manager.</td>
</tr>
<tr>
<td><strong>Unlink agents that have</strong></td>
<td>Tenable.io automatically tracks unlinked agents and related data for the number of days specified in this option. You cannot turn off this tracking.</td>
</tr>
<tr>
<td>been inactive for X days</td>
<td></td>
</tr>
</tbody>
</table>
| **Override Blackout Windows** | When enabled, this option overrides scheduled blackout windows. It prevents agents from receiving software updates at any time.  
  Agents continue to receive plugin updates and perform scheduled scans. |

**Note:** Inactive agents that were automatically unlinked by Tenable.io do not automatically relink if they come back online.
Modify Agent Settings (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to modify agent settings in Tenable.io.

To modify agent settings:

1. In the top navigation bar, click **Scans**.
   - The **My Scans** page appears.
2. In the left navigation bar, click **Agents**.
   - The **Agents** page appears.
3. Click the **Agent Settings** tab.
4. Modify the **settings** as necessary.
5. Click **Save**.
   - The manager saves your changes.
Agent Status (Classic Interface)

Nessus Agents can be in one of the following statuses:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online</td>
<td>The host that contains the Nessus Agent is currently connected and in com-</td>
</tr>
<tr>
<td></td>
<td>munication with Tenable.io.</td>
</tr>
<tr>
<td>Offline</td>
<td>The host that contains the Nessus Agent is currently powered down or not con-</td>
</tr>
<tr>
<td></td>
<td>nected to a network.</td>
</tr>
<tr>
<td>Initializing</td>
<td>The Nessus Agent is in the process of checking in with Tenable.io.</td>
</tr>
</tbody>
</table>
Filter Agents (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to filter agents in Tenable.io (classic interface).

To filter agents in the agents table in Tenable.io:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Agents**.
   
   The **Agents** page appears.

3. Above the agents table, click the **Filter** button.
   
   The **Filter** window appears.

4. Configure the filters as necessary. For more information, see **Agent Filters**.

5. Click **Apply**.

   The manager filters the list of agents to include only those that match your configured options.

### Agent Filters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Operator</th>
<th>Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>is equal to</td>
<td>In the text box, type the IPv4 or IPv6 addresses on which you want to filter.</td>
</tr>
<tr>
<td></td>
<td>is not equal to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>contains</td>
<td></td>
</tr>
<tr>
<td></td>
<td>does not contain</td>
<td></td>
</tr>
<tr>
<td>Last Connection</td>
<td>earlier than</td>
<td>In the text box, type the date on which you want to filter.</td>
</tr>
<tr>
<td></td>
<td>later than</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Operator</td>
<td>Expression</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last Plugin Update</td>
<td>on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>not on</td>
<td></td>
</tr>
<tr>
<td>Last Scanned</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member of Group</td>
<td>is equal to</td>
<td>From the drop-down list, select from your existing agent groups.</td>
</tr>
<tr>
<td></td>
<td>is not equal to</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>is equal to</td>
<td>In the text box, type the agent name on which you want to filter.</td>
</tr>
<tr>
<td></td>
<td>is not equal to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>contains</td>
<td></td>
</tr>
<tr>
<td></td>
<td>does not contain</td>
<td></td>
</tr>
<tr>
<td>Platform</td>
<td>contains</td>
<td>In the text box, type the platform name on which you want to filter.</td>
</tr>
<tr>
<td></td>
<td>does not contain</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>is equal to</td>
<td>In the drop-down list, select an <a href="#">agent status</a>.</td>
</tr>
<tr>
<td></td>
<td>is not equal to</td>
<td></td>
</tr>
<tr>
<td>Version</td>
<td>is equal to</td>
<td>In the text box, type the version you want to filter.</td>
</tr>
<tr>
<td></td>
<td>is not equal to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>contains</td>
<td></td>
</tr>
<tr>
<td></td>
<td>does not contain</td>
<td></td>
</tr>
</tbody>
</table>
Unlink an Agent (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

When you manually unlink an agent, the agent disappears from the **Agents** page, but the system retains related data for the period of time specified in **agent settings**. When you manually unlink an agent, the agent does *not* automatically relink to Tenable.io.

**Tip:** You can configure agents to automatically unlink if they are inactive for a certain number of days, as described in **agent settings**.

To manually unlink agents in Nessus Manager:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Agents**.
   
   The **Agents** page appears.

3. Do one of the following:
   
   • To unlink a single agent:
     
     a. In the agents table, in the row for the agent that you want to unlink, click the ✗ button.
     
     A confirmation window appears.
   
   • To unlink multiple agents:
     
     a. In the agents table, select the check box in each row for each agent you want to unlink.
     
     b. In the upper-right corner, click **Unlink**.
     
     A confirmation window appears.

4. Click the **Unlink** button.
   
   The manager unlinks the agent.

To manually unlink agents in Tenable.io:
Required Tenable.io Vulnerability Management User Role: Scan Manager or Administrator

1. In the upper-left corner, click the button.
   The left navigation plane appears.

2. In the left navigation plane, click Settings.
   The Settings page appears.

3. Click the Sensors tile.
   The Sensors page appears. By default, Nessus Scanners is selected in the left navigation menu and the Cloud Scanners tab is active.

4. In the left navigation menu, click Agents.
   The Agents page appears and the Linked Agents tab is active.

5. (Optional) Search for a specific agent or filter the agents in the table. For filter descriptions, see Agent Filters.

6. Do one of the following:
   - In the agents table, select the check box next to each agent you want to restart.
   - In the table header, select the check box to select the entire page.

   An action bar appears at the bottom of the page.

   **Tip:** In the action bar, select Select All Pages to select all linked agents.

7. Click the button.
   A confirmation window appears.

8. Click the Unlink button.
   Tenable.io unlinks the agents.
Export Agents (Classic Interface)

To export agents data in Tenable.io:

1. In the top navigation bar, click **Scans**.
   
The **My Scans** page appears.

2. In the left navigation bar, click **Agents**.
   
The **Agents** page appears.

3. In the upper right corner, click **Export**. If a drop-down appears, click **CSV**.
   
   Your browser’s download manager appears.

4. Click **OK** to save the agents.csv file.

The agents.csv file exported from Tenable.io contains the following data:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Name</td>
<td>The name of the agent.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the agent at the time of export. Possible values are unlinked, online, or offline.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IPv4 or IPv6 address of the agent.</td>
</tr>
<tr>
<td>Platform</td>
<td>The platform the agent is installed on.</td>
</tr>
<tr>
<td>Groups</td>
<td>The names of any groups the agent belongs to.</td>
</tr>
<tr>
<td>Group IDs</td>
<td>The group IDs of any groups the agent belongs to.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the agent.</td>
</tr>
<tr>
<td>Last Plugin Update</td>
<td>The date (in ISO-8601 format) the agent's plugin set was last updated.</td>
</tr>
<tr>
<td>Agent ID</td>
<td>The ID of the agent.</td>
</tr>
<tr>
<td>Agent UUID</td>
<td>The UUID of the agent.</td>
</tr>
<tr>
<td>Linked On</td>
<td>The date (in ISO-8601 format) the agent was linked to Tenable.io.</td>
</tr>
<tr>
<td>----------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last Connect</td>
<td>The date (in ISO-8601 format) of the agent's last check-in.</td>
</tr>
<tr>
<td>Last Scanned</td>
<td>The date (in ISO-8601 format) the agent was last scanned.</td>
</tr>
</tbody>
</table>
Download Linked Agent Logs (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

In Tenable.io, you can request and download a log file containing logs and system configuration data from any of your managed scanners and agents. This information can help you troubleshoot system problems, and also provides an easy way to gather data to submit to Tenable Support.

You can store a maximum of five log files from each agent in Tenable.io. Once the limit is reached, you must remove an old log file to download a new one.

To download logs from a linked agent in Tenable.io:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.
2. In the left navigation bar, click **Agents**.
   
   The **Agents** page appears.
3. In the agents table, click the agent for which you want to download logs.
   
   The **Agents** page for that agent appears.
4. Click the **Logs** tab.
5. In the upper-right corner, click **Request Logs**.

   **Note:** If you have reached the maximum of five log files, the **Request Logs** button is disabled. Remove an existing log before downloading a new one.

   The manager requests the logs from the agent the next time it checks in, which may take several minutes. You can view the status of the request in the user interface until the download is complete.
6. To download the log file, click the file name.
   
   Your system downloads the log file.

To remove an existing log:
In the row of the log you want to remove, click the button.

To cancel a pending or failed log download:

In the row of the pending or failed log download that you want to cancel, click the button.
Agent Groups (Classic Interface)

You can use agent groups to organize and manage the agents linked to your Tenable.io. You can add an agent to more than one group, and configure scans to use these groups as targets.

To manage agent groups, use the following procedures:

- [Create an Agent Group (Classic Interface)]
- [Configure User Permissions for an Agent Group]
- [Modify an Agent Group (Classic Interface)]
- [Delete an Agent Group (Classic Interface)]
Create an Agent Group (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

You can use agent groups to organize and manage the agents linked to your account. You can add an agent to more than one group, and configure scans to use these groups as targets.

Use this procedure to create an agent group in Tenable.io (classic interface).

To create a new agent group in Tenable.io:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Agents**.
   
   The **Agents** page appears.

3. Click the **Agent Groups** tab.

4. In the upper right corner, click the **New Group** button.
   
   The **New Agent Group** window appears.

5. In the **Name** box, type a name for the new agent group.

6. (Optional) Add agents to the group:
   
   a. Click the **Add Members** toggle.
      
      A list of linked agents appears.
   
   b. Click each agent you want to add to the group.

7. Click **Save**.

   The manager adds the agent group and it appears in the table.

What to do next:

- **Configure** user permissions for the agent group.
- **Use** the agent group in an agent scan configuration.
Configure User Permissions for an Agent Group (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

You can share an agent group with other users or user groups in your organization.

User permissions for agent groups include the following:

- **No access** – (Default user only) The user or user group cannot add the agent group to an agent scan. If a user or user group with this permission attempts to launch an existing scan that uses the agent group, the scan fails.

- **Can use** – The user or user group can add the agent group to an agent scan and can launch existing scans that use the agent group.

Use this procedure to configure permissions for an agent group in Tenable.io.

To configure user permissions for an agent group:

1. Create or modify an agent group.

2. In the agent groups table, click the agent group for which you want to configure permissions.

   The agent group details page appears.

3. Click the **Permissions** tab.

   The **Permissions** tab appears.

4. Do any of the following:

   - **Tip:** Tenable recommends assigning permissions to user groups, rather than individual users, to minimize maintenance as individual users leave or join your organization.

   - Add permissions for a new user or user group:
     a. In the **Add users or groups** box, type the name of a user or group.

        As you type, a filtered list of users and groups appears.

     b. Select a user or group from the search results.
Tenable.io adds the user to the permissions list, with a default permission of Can Use.

- **Change the permissions for an existing user or user group:**
  
  **Note:** The Default user represents any users who have not been specifically added to the agent group.
  
  a. Next to the permission drop-down for the Default user, click the ▼ button.
  
  b. Select a permissions level.
  
  c. Click **Save**.

- **Remove permissions for a user or user group:**
  
  • For the Default user, set the permissions to **No Access**.
  
  • For any other user or user group, click the ✗ button next to the user or user group for which you want to remove permissions.

5. Click **Save**.

Tenable.io saves the changes you made to the agent group.
Modify an Agent Group (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to modify an agent group in Tenable.io (classic interface).

To modify an agent group in Tenable.io:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Agents**.

   The **Agents** page appears.

3. Click the **Agent Groups** tab.

4. Do any of the following:

   - **Modify the group name.**
     
     a. In the row for the agent group that you want to modify, click the **edit** button.

        The **Edit Agent Group** window appears.

     b. In the **Name** box, type a new name for the agent group.

     c. Click **Save**.

        The manager saves your changes.

   - **Add agents to the agent group.**
     
     a. In the agent groups table, click the agent group you want to modify.

        The agent group details page appears.

     b. In the upper-right corner of the page, click the **Add Members** button.

        The **Add Members** window appears. This window contains a table of available agents.
c. (Optional) In the **Search** box, type the name of an agent, then click **Enter**.

   The table of agents refreshes to display the agents that match your search criteria.

d. Click the check box next to each agent you want to add to the group.

e. Click **Add**.

   The manager adds the selected agent or agents to the group.

**Remove agents from the agent group.**

a. In the agent groups table, click the agent group you want to modify.

   The agent group details page appears. By default, the **Members** tab is active.

b. (Optional) Filter the agent groups in the table.

c. (Optional) Search for an agent by name.

d. Select the agent or agents you want to remove:
   
   - For an individual agent, click the **X** button next to the agent.
   
   - For multiple agents, select the check box next to each, then click the **Remove** button in the upper-right corner of the page.

   A confirmation window appears.

e. In the confirmation window, confirm the removal.

**Modify the user permissions for the agent group.**

a. In the agent groups table, click the agent group you want to modify.

   The agent group details page appears.

b. Click the **Permissions** tab.

   The **Permissions** tab appears.

c. **Configure** the user permissions for the group.
Delete an Agent Group (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to delete an agent group in Tenable.io.

To delete an agent group in Tenable.io:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Agents**.
   
   The **Agents** page appears.

3. Click the **Groups** tab.

4. In the row for the agent group that you want to delete, click the \( \times \) button.
   
   A confirmation window appears.

5. To confirm, click **Delete**.
   
   The manager deletes the agent group.
Blackout Windows (Classic Interface)

Blackout windows allow you to schedule times where certain agent activities are suspended for all linked agents. This activity includes:

- Receiving and applying software updates

Blackout windows do not prevent linked agents from:

- Receiving plugin updates
- Installing or executing agent scans

To manage blackout freeze windows, use the following procedures:

- [Create a Blackout Window](#)
- [Modify a Blackout Window](#)
- [Delete a Blackout Window](#)
Create a Blackout Window (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Blackout windows allow you to schedule times where certain agent activities are suspended for all linked agents. This activity includes:

- Receiving and applying software updates

Blackout windows do not prevent linked agents from:

- Receiving plugin updates
- Installing or executing agent scans

To create a blackout window for linked agents in Tenable.io:

1. In the top navigation bar, click **Scans**.
   - The **My Scans** page appears.
2. In the left navigation bar, click **Agents**.
   - The **Agents** page appears.
3. Click the **Blackout Windows** tab.
4. In the upper-right corner, click the **New Window** button.
   - The **New Blackout Window** page appears.
5. Configure the options as necessary.
6. Click **Save**.
   - The blackout window goes into effect and appears on the **Blackout Windows** tab.
Modify a Blackout Window (Classic Interface)

Required Tenable.io Vulnerability Management User Role: Scan Manager or Administrator

Use this procedure to modify a blackout window in Tenable.io (classic interface).

To configure global blackout window settings, see Agent Settings.

To modify a blackout window in Tenable.io:

1. In the top navigation bar, click Scans.
   
   The My Scans page appears.

2. In the left navigation bar, click Agents.

   The Agents page appears.

3. Click the Blackout Windows tab.

4. In the blackout windows table, click the blackout window you want to modify.

   The blackout window details page appears.

5. Modify the options as necessary.

6. Click Save to save your changes.
Delete a Blackout Window (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to delete a blackout window in Tenable.io (classic interface).

To delete a blackout window for linked agents in Tenable.io:

1. In the top navigation bar, click **Scans**.
   
   The **My Scans** page appears.

2. In the left navigation bar, click **Agents**.
   
   The **Agents** page appears.

3. Click the **Blackout Windows** tab.

4. In the blackout window table, in the row for the blackout window that you want to delete, click the ✗ button.
   
   A dialog box appears, confirming your selection to delete the blackout window.

5. Click **Delete** to confirm the deletion.

   The manager deletes the blackout window.
### Settings

You can access **Settings** for Tenable.io in the **new interface** or in the **classic interface**.

<table>
<thead>
<tr>
<th>Settings Page</th>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>New</td>
<td>Manage SLA and severity settings.</td>
</tr>
<tr>
<td>About</td>
<td>New or Classic</td>
<td>View information about Tenable.io.</td>
</tr>
<tr>
<td>Recast and Accept</td>
<td>New or Classic</td>
<td>Manage recast and accept rules.</td>
</tr>
<tr>
<td>Rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tags</td>
<td>New or Classic</td>
<td>Manage asset tags.</td>
</tr>
<tr>
<td>Connectors</td>
<td>New</td>
<td>Manage connectors.</td>
</tr>
<tr>
<td>Managed Credentials</td>
<td>New</td>
<td>Configure managed credentials.</td>
</tr>
<tr>
<td>Access Groups</td>
<td>New</td>
<td>Manage access groups.</td>
</tr>
<tr>
<td>My Account</td>
<td>New or Classic</td>
<td>Manage your own user account.</td>
</tr>
<tr>
<td>Users</td>
<td>New or Classic</td>
<td>Manage accounts for other users.</td>
</tr>
<tr>
<td>Groups</td>
<td>New or Classic</td>
<td>Manage user groups.</td>
</tr>
<tr>
<td>Sensors</td>
<td>New</td>
<td>Manage sensors, including agents.</td>
</tr>
</tbody>
</table>

**Note:** For sensors and agents in the classic interface, see [Scanners](#) and [Agents](#).
On the **General** page, you can configure general settings for your Tenable.io instance. For more information, see:

- [Configure Your Severity Metric](#)
- [Configure Your SLA Settings](#)
- [Change the Language for Plugin Details](#)
Configure Your Severity Metric

**Required User Role:** Administrator

By default, Tenable.io uses CVSSv2 scores to calculate severity for individual vulnerability instances. If you want Tenable.io to calculate the severity of vulnerabilities using CVSSv3 scores (when available), you can configure your severity metric setting.

**Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

For information about severity and the ranges for CVSSv2 and CVSSv3, see [CVSS vs. VPR](#).

**Note:** This setting does not affect the calculations displayed in the **SLA Progress: Vulnerability Age** widget. To modify your SLA severity, see [Configure Your SLA Settings](#).

To configure your severity setting in the new interface:

1. In the upper-left corner, click the □ button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **General** tile.
   
   The **General** page appears. By default, the **Severity** tab is active.

4. Select the metric that you want Tenable.io to use for severity calculations.
   
   - **CVSSv2** – Use CVSSv2 scores for all severity calculations.
   
     - **CVSSv3** – Use CVSSv3 scores, when available, for all severity calculations. Use CVSSv2 only if a CVSSv3 score is not available.

5. Click **Save**.

6. The system saves your change and begins calculating severity based on your selection.

All vulnerabilities seen before the change retain their severity. After the change, all vulnerabilities seen during scans receive severities based on your new selection. Because of this,
you could see two sightings of the same vulnerability have two different CVSS scores and severities.

**Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.
Configure Your SLA Settings

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can configure Service Level Agreement (SLA) settings to modify how Tenable calculates your SLA data.

You can view this data in the **SLA Progress: Vulnerability Age** widget on the **Vulnerability Management Overview** dashboard. For more information, see [Vulnerability Management Overview Dashboard](#).

**Note:** This section describes the new interface. For information about the classic interface, see [My Account (Classic Interface)](#). For information about navigating the new interface, see [Navigate Tenable.io (New Interface)](#).

To configure your SLA settings in the new interface:

1. In the upper-left corner, click the **button.**
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **General** tile.
   
   The **General** page appears. By default, the **Severity** tab is active.

4. Configure the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Default</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Age SLA</td>
<td>• <strong>Critical</strong> 7 days</td>
<td>• To exclude a severity from your SLA data, clear the check box next to <strong>Critical</strong>, <strong>High</strong>, <strong>Medium</strong>, or <strong>Low</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>High</strong> 30 days</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Medium</strong> 60</td>
<td>• To modify the number of days included for each severity, type an integer in the box</td>
</tr>
<tr>
<td>Override Vulnerability Severity Metric</td>
<td>VPR</td>
<td>Specifies whether Tenable uses VPR severity, CVSSv2 severity, or CVSSv3 severity to calculate SLA data. For more information about these metrics, see CVSS vs. VPR.</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----</td>
<td>------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Vulnerability Age Metric</td>
<td>First Seen</td>
<td>Specifies whether Tenable uses <strong>First Seen</strong> or <strong>Published Date</strong> to calculate SLA data.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

Tenable.io saves your SLA settings.
Change the Language for Plugin Details

**Required User Role:** Administrator

You can configure the language in which plugin details appear in the Tenable.io Vulnerability Management workspace.

**Note:** By default, the plugin details language selection is only available for users in the jp01 site in the APAC cloud sensor region. To request this feature in other APAC region sites, contact your Tenable representative.

**Note:** The plugin details language selection affects all user accounts in your Tenable.io instance.

**Note:** Upating this setting does not update the plugin language for historical scan results. You must re-run a scan to view the results in the selected plugin language.

**Note:** If you export plugin data in .cvs format to use in Microsoft Excel, ensure the selected language in Microsoft Excel matches your plugin details language.

To change the plugin details language in the new interface:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **General** tile.

   The **General** page appears. By default, the **Severity** tab is active.

4. In the left navigation plane, click the **Language** tab.

   The language options appear.

5. In the **Language** drop-down box, select the language you want to use for plugin details in the Tenable.io Vulnerability Management workspace.

6. Click **Save**.
Tenable.io saves your settings and updates the language for all user accounts in your Tenable.io instance.
View Information about Your Tenable.io Instance

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Note:** This section describes the new interface. For information about the classic interface, see [View Information about Your Tenable.io Instance (Classic Interface)](#). For information about navigating the new interface, see [Navigate Tenable.io (New Interface)](#).

The **License** page contains information about your Tenable.io instance, including license and environment details. For more information about how licenses are counted or reclaimed, see [Tenable.io Vulnerability Management Licenses](#) and [Tenable.io Web Application Scanning Licenses](#).

To view details about your Tenable.io instance and license:

1. In the upper-left corner, click the **☰** button.

   The left navigation plane appears.

2. Click **Settings**.

   The **Settings** page appears.

3. Click the **License** tile.

   The **License** page appears.

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Overview (90 Days)</td>
<td>The ring chart visualizes your licensed asset usage by product. The count next to the chart summarizes your licensed assets currently in use compared to your total licensed amount. The counts to the right of the chart provide a more detailed asset count breakdown by:</td>
<td>Click the widget to view the licensed assets in the <strong>Assets</strong> plane for further analysis or to configure scanning for discovered assets.</td>
</tr>
</tbody>
</table>
- **Product license** — The number of assets associated with each individual product license. For example, if you have a Tenable.ep license, you see a count for your licensed assets currently in use and platform-specific counts for each contributing Tenable.io product.

- **Discovered Assets** — The number of discovered assets (not assessed) within the last 90 days.

- **Deleted Assets** — The number of assets deleted within the last 90 days.

| Licensed Assets By Scan Source (90 Days) | The number of licensed assets by scan source. | Click a row in the table to view the licensed assets in the Assets plane, filtered by scan source. |
| License Expiration | The type of license, the amount of time remaining on the license, and the expiration date for the license. | None. |
| Environment Information | Information about the region in which your Tenable.io container resides and its container ID. Additionally, this widget contains information about your Vulnerability Management plugin set and the last time the plugins were updated. | None. |

**Tip:** Your site is a geographical location that corresponds with your region. You can provide this information directly to Tenable Support when reporting a potential issue.
View Information about Your Tenable.io Instance (Classic Interface)

Required Tenable.io Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

To access the About page, in the top navigation bar, click Settings. The About page appears.

The About page contains information about your Tenable.io instance. Depending on your user role, this page can contain the following:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable.io License (Administrators only)</td>
<td></td>
</tr>
<tr>
<td>Licensed Assets</td>
<td>The number of assets that are licensed to be used with the instance.</td>
</tr>
<tr>
<td>Expiration</td>
<td>The date on which your license expires.</td>
</tr>
<tr>
<td>Plugins</td>
<td></td>
</tr>
<tr>
<td>Last Updated</td>
<td>The date on which the plugin set for the instance was last refreshed.</td>
</tr>
<tr>
<td>Plugin Set</td>
<td>The ID of the current plugin set.</td>
</tr>
<tr>
<td>Tenable.io Region</td>
<td></td>
</tr>
<tr>
<td>Region</td>
<td>The region of the Tenable.io instance.</td>
</tr>
</tbody>
</table>
Recast/Accept Rules

Note: This section describes the new interface. For information about the classic interface, see Recast Rules (Classic Interface). For information about navigating the new interface, see Navigate Tenable.io (New Interface).

Note: If a rule is targeted by IP address, that rule applies to the specified IP in each network in which it is found. For more information, see networks.

Recast Rules

You can use recast rules to modify the severity of vulnerabilities. Vulnerabilities that you recast are identified as such on the Vulnerability Details page. If you specify an expiration date for a recast rule, upon expiration Tenable.io reverts existing dashboards back to their original severity. Historical scan results, however, remain unchanged.

For example, you may have a set of internal servers that you scan regularly. These internal servers use self-signed certificates for SSL connections. Since the certificates are self-signed, your scans have been reporting vulnerabilities from plugin 51192, SSL Certificate Cannot Be Trusted, which has a Medium severity. Since you are aware that the servers use self-signed certificates, you create a recast rule to change the severity level of plugin 51192 from Medium to Info, and set the target to those internal servers.

The dashboards reflect the effect of a recast rule. A tag appears to indicate when vulnerabilities have been recast. The rule applies to all assets or a specific asset based on the rule’s parameters. As long as the rule remains in effect, the rule applies to the corresponding data and scan results.

Note: While recasting NNM plugins, the original severity is unknown.

Note: Upon creation, recast rules do not apply to historical scan results; however, they do apply to existing data in Tenable.io.

Note: Because PCI ASV scans using the PCI Quarterly External Scan template have their own set of rules, any recast rules do not apply to the scan results.

Accept Rules
You can use accept rules to accept the risk of a vulnerability without modifying the severity level of the plugin. Vulnerabilities that have been accepted are still identified by a scan, but hidden in the results of the scan. To view accepted vulnerabilities, you can use the Recast & Accept filter. If you specify an expiration date for an accept rule, upon expiration Tenable.io no longer accepts the risk of the vulnerability. Historical scan results, however, remain unchanged.

Consider the previous example. Rather than recasting the severity level from Medium to Info, you acknowledge that there is a risk associated with using self-signed certificates, but you do not want to see the vulnerability appearing for those servers any longer. You create an accept rule to accept the risk of plugin 51192, which hides that vulnerability for the targets you specified. If the same vulnerability is identified on other assets during the scan, those still appear in the scan results.

Tenable.io reflects the effect of an accept rule. Accepted vulnerabilities are hidden, and can be viewed using the Recast & Accepted filter.

False Positives

Additionally, you can use an accept rule to report false positives. Tenable reviews reported false positives in order to identify potential issues with a plugin.

Consider again the previous example. In this case, you know the servers in question are in fact using certificates from a proper Certificate Authority. However, plugin 51192 continues to report vulnerabilities for those servers. To hide the false results and report the issue, you create an accept rule that accepts the vulnerability as a false positive.

Integrity of Scan History

In the case of both recast and accept rules, the historical results of a scan are not modified. Scan history is immutable in order to provide an accurate representation of the scan over time, and to prevent any internal or external auditing issues that might be created by the scan history changing.

For information on using Recast/Accept rules, see:

- [View Recast/Accept Rules](#)
- [Create a Recast Rule](#)
- [Create an Accept Rule for a Plugin](#)
• Edit a Recast or Accept Rule
• Delete a Recast or Accept Rule
View Recast/Accept Rules

**Required User Role:** Administrator

The **Recast/Accept Rules** page displays all configured recast and accept rules in your Tenable.io instance.

To view the **Recast/Accept Rules** page:

1. In the upper-left corner, click the menu button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Recast** tile.
   
   The **Recast/Accept Rules** page appears.
Create a Recast Rule

**Required User Role:** Administrator

**Note:** You can also create a recast rule [directly from the Vulnerability Details page](#).

To create a recast rule:

1. **View** the Recast/Accept Rules page.
2. In the upper-right corner, click the **Add Rule** button.
   
   The **Rule** plane appears.
3. In the **Action** section, select **Recast**.
4. In the **Vulnerability** box, type the ID of the plugin that you want to recast. For example, 51192.

   **Note:** If the plugin ID corresponds to a Nessus plugin, the **Original Severity** indicator changes to match the default severity of the vulnerability. The **Original Severity** indicator does not change if another type of plugin is used.

5. In the **New Severity** drop-down box, select the severity level for the vulnerability.
6. In the **Targets** drop-down box, do one of the following:
   
   - To target all assets, select **All**. This is the default target.

     **Note:** If the **Targets** drop-down is set to **All**, a warning appears indicating that this option may override existing rules.

   - To target a custom set of assets:
     a. Select **Custom**.

        A **Target Hosts** box appears.

     b. In the **Target Hosts** box, type one or more targets for the rule.

        You can type a comma-delimited list that includes any combination of IP addresses, IP ranges, CIDR, and hostnames.
7. (Optional) In the **Expires** box, set an expiration date for the rule. This action is only necessary if you want the rule to expire. By default, the rule applies indefinitely.

8. (Optional) In the **Comments** box, type a description of the rule. The text you type in this box is only visible if the rule is modified and has no functional effect.

9. Click **Save**.

   Tenable.io starts applying the rule to existing vulnerabilities. This process may take some time, depending on the system load and the number of matching vulnerabilities. The change is reflected on dashboards, where a label appears to indicate how many instances of affected vulnerabilities have been recast.

   **Note:** A recast rule does not affect the historical results of a scan.
Create an Accept Rule for a Plugin

**Required User Role:** Administrator

**Note:** You can also create a recast rule directly from the Vulnerability Details page.

To create an accept rule:

1. View the Recast/Accept Rules page.
2. In the upper-right corner, click the Add Rule button.
   
   The Rule plane appears.
3. In the Action section, select Accept.
4. In the Vulnerability box, type the ID of the plugin that you want to recast. For example, 51192.
   
   **Note:** If the plugin ID corresponds to a Nessus plugin, the Original Severity indicator changes to match the default severity of the vulnerability. The Original Severity indicator does not change if another type of plugin is used.
5. In the Targets drop-down box, do one of the following:
   
   - To target all assets, select All. This is the default target.
   - To target a custom set of assets:
     
     a. Select Custom.

     A Target Hosts box appears.

     b. In the Target Hosts box, type one or more targets for the rule.

     You can type a comma-delimited list that includes any combination of IP addresses, IP ranges, CIDR, and hostnames.
6. (Optional) In the Expires box, set an expiration date for the rule. This action is only necessary if you want the rule to expire. By default, the rule applies indefinitely.
7. (Optional) In the Comments box, type a description of the rule. The text you type in this box is only visible if the rule is modified and has no functional effect.
8. (Optional) To report the vulnerability as a false positive:

   a. Enable the **Report as false positive** toggle.

      A **Message To Tenable** box appears.

   b. In the **Message to Tenable** box, type a description of the false positive to send to Tenable.

9. Click **Save**.

   Tenable.io starts applying the rule to existing vulnerabilities. This process may take some time, depending on the system load and the number of matching vulnerabilities. The affected vulnerability is hidden on your workbench.

   **Note:** To view vulnerabilities hidden from your workbench, use the **Recast & Accept** advanced filter.
Edit a Recast or Accept Rule

**Required User Role:** Administrator

To edit a recast or accept rule:

1. **View** the *Recast/Accept Rules* page.

2. In the *Recast/Accept Rules* table, click the row of the rule you want to edit.
   
   The *Rule* plane appears.

3. Make any desired changes.
   
   For more information about configuration options, see [Create a Recast Rule](#) or [Create an Accept Rule for a Plugin](#).

4. Click **Save**.
   
   Tenable.io applies your changes to the rule. This process may take some time, depending on the system load and the number of matching vulnerabilities.
Delete a Recast or Accept Rule

Required User Role: Administrator

To delete a recast or accept rule:

1. View the Recast/Accept Rules page.

2. Select a rule or rules to delete:
   - Select a single rule.
     a. In the Recast/Accept Rules table, roll over the row of the rule you want to delete.
     b. On the right side of the row, click the button.

       A Delete Recast Rule confirmation message appears.

   - Select multiple rules.
     a. In the Recast/Accept Rules table, select the check boxes next to the rules you want to delete.

       The action bar appears at the bottom of the page.
     b. In the action bar, click the button.

       A Delete Recast Rule confirmation message appears.

3. Click Delete.

   Tenable.io deletes the selected rule or rules. Tenable.io may take some time to remove the rule or rules from existing vulnerabilities, depending on the system load and the number of matching vulnerabilities.
Recast Rules (Classic Interface)

**Note:** The Recast Rules feature replaces the Plugin Rules feature. Any existing plugin rules are migrated to recast rules.

**Note:** If a rule is targeted by IP, that rule applies to the specified IP in each network in which it is found. For more information, see networks.

Recast Rules

You can use recast rules to modify the severity of vulnerabilities. Vulnerabilities that you recast are identified as such on the Vulnerability Details page. If you specify an expiration date for a recast rule, upon expiration Tenable.io reverts existing dashboards back to their original severity. Historical scan results, however, remain unchanged.

For example, you may have a set of internal servers that you scan regularly. These internal servers use self-signed certificates for SSL connections. Since the certificates are self-signed, your scans have been reporting vulnerabilities from plugin 51192, SSL Certificate Cannot Be Trusted, which has a Medium severity. Since you are aware that the servers use self-signed certificates, you create a recast rule to change the severity level of plugin 51192 from Medium to Info, and set the target to those internal servers.

The workbenches reflect the effect of a recast rule. A tag appears to indicate when vulnerabilities have been recast. The rule applies to all assets or a specific asset based on the rule’s parameters. As long as the rule remains in effect, the rule applies to the corresponding data and scan results.

**Note:** While recasting NNM plugins, the original severity is unknown.

**Note:** Upon creation, recast rules do not apply to historical scan results; however, they do apply to existing data in Dashboard and Workbench views.

Accept Rules

You can use accept rules to accept the risk of a vulnerability without modifying the severity level of the plugin. Vulnerabilities that have been accepted are still identified by a scan, but hidden in the results of the scan. To view accepted vulnerabilities, you can use the Recast & Accept filter. If you spe-
Cify an expiration date for an accept rule, upon expiration Tenable.io no longer accepts the risk of the vulnerability. Historical scan results, however, remain unchanged.

Consider the previous example. Rather than recasting the severity level from Medium to Info, you acknowledge that there is a risk associated with using self-signed certificates, but you do not want to see the vulnerability appearing for those servers any longer. You create an accept rule to accept the risk of plugin 51192, which hides that vulnerability for the targets you specified. If the same vulnerability is identified on other assets during the scan, those still appear in the scan results.

The workbenches reflect the effect of an accept rule. Accepted vulnerabilities are hidden, and can be viewed using the Recast & Accepted filter.

False Positives

You can use an accept rule to report false positives. Tenable, Inc. reviews reported false positives in order to identify potential issues with a plugin.

Consider again the previous example. In this case, you know the servers in question are in fact using certificates from a proper Certificate Authority. However, plugin 51192 continues to report vulnerabilities for those servers. To hide the false results and report the issue, you create an accept rule that accepts the vulnerability as a false positive.

Integrity of Scan History

In the case of both recast and accept rules, the historical results of a scan are not modified. Scan history is immutable in order to provide an accurate representation of the scan over time, and to prevent any internal or external auditing issues that might be created by the scan history changing.

For information on using Recast/Accept rules, see:

- [View Recast/Accept Rules (Classic Interface)]
- [Create a Recast Rule (Classic Interface)]
- [Edit a Recast Rule (Classic Interface)]
- [Delete a Recast Rule (Classic Interface)]
- [Create an Accept Rule (Classic Interface)]
• Edit an Accept Rule (Classic Interface)
• Delete an Accept Rule (Classic Interface)
View Recast/Accept Rules (Classic Interface)

**Required User Role:** Administrator


To access the Recast Rules page:

1. In the top navigation bar, click **Settings**.
2. In the left navigation bar, click **Recast Rules**.

The Recast Rules page appears.

Recast rules allow you to accept or modify the severity of a given vulnerability. In addition, rules can be limited to a specific asset or specific time frame. From this page you can view, create, edit, and delete your rules.
Create a Recast Rule (Classic Interface)

**Required User Role:** Administrator

To create a recast rule:

1. In the top navigation bar, click **Settings**.
   
   The **About** page appears.

2. In the left navigation bar, click **Recast Rules**.
   
   The **Recast Rules** page appears.

3. Click **New Rule**.
   
   The **New Recast Rule** page appears.
4. In the **Target Vulnerability** box, type the ID of the plugin that you want to recast. For example, 51192.

   **Note:** If the plugin ID corresponds to a Nessus plugin, the **Original Severity** indicator changes to match the default severity of the vulnerability. The **Original Severity** indicator does not change if another type of plugin is used.

5. In the **Set to** box, select the severity level for the vulnerability.

6. In the **Target** box, do one of the following:
- To target all assets, select **All**. This is the default target.

- To target a custom set of assets:
  
  a. Select **Custom**.

  A text box appears.

  b. In the text box, type one or more targets for the rule.

  You can type a comma-delimited list that includes any combination of IP addresses, IP ranges, CIDR, and hostnames.

7. (Optional) In the **Expiration** box, set an expiration date for the rule. This action is only necessary if you want the rule to expire. By default, the rule applies indefinitely.

8. (Optional) In the **Comments** box, type a description of the rule. The text you type in this box is only visible if the rule is modified and has no functional effect.

9. Click **Save**.

   Tenable.io starts applying the rule to existing vulnerabilities. This process may take some time, depending on the system load and the number of matching vulnerabilities. The change is reflected on your workbench, where a label appears to indicate how many instances of affected vulnerabilities have been recast.

   **Note:** A recast rule does not affect the historical results of a scan.
Edit a Recast Rule (Classic Interface)

**Required User Role:** Administrator

To edit a recast rule:

1. In the top navigation bar, click **Settings**.
   
   The *About* page appears.

2. In the left navigation bar, click **Recast Rules**.
   
   The *Recast Rules* page appears.

3. In the recast rules table, click the rule you want to edit.
   
   The *Edit Recast Rule* page appears.
4. Make any changes to the rule.

5. Click **Save**.

   Tenable.io saves the changes to the rule. Tenable.io may take some time to apply the changes to the rule and existing vulnerabilities, depending on the system load and the number of matching vulnerabilities.
Delete a Recast Rule (Classic Interface)

**Required User Role:** Administrator

**Note:** When a rule is deleted or expires, the rule is reversed, and the change is reflected in the workbench.

To delete a recast rule:

1. In the top navigation bar, click **Settings**.
   
   The **About** page appears.

2. In the left navigation bar, click **Recast Rules**.
   
   The **Recast Rules** page appears.

   ![Recast Rules Table](image)

   - **Action** column allows you to accept or modify the severity of a given vulnerability. In addition, rules can be limited to a specific asset or specific time frame. From this page you can view, create, edit, and delete your rules.

<table>
<thead>
<tr>
<th>Action</th>
<th>Vulnerability</th>
<th>Plugin ID</th>
<th>Old Sev</th>
<th>New Sev</th>
<th>Targets</th>
<th>Expiration</th>
<th>Date Created</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>SSL Certificate Cannot Be Trusted</td>
<td>511192</td>
<td>Medium</td>
<td>N/A</td>
<td>All Assets</td>
<td>N/A</td>
<td>07/10/17</td>
<td><a href="mailto:screenshots@tenable.admin">screenshots@tenable.admin</a></td>
</tr>
<tr>
<td>Recast</td>
<td>SSH Weak Algorithm Supported</td>
<td>96017</td>
<td>Medium</td>
<td>Critical</td>
<td>172.26.68.104</td>
<td>N/A</td>
<td>07/07/17</td>
<td><a href="mailto:screenshots@tenable.admin">screenshots@tenable.admin</a></td>
</tr>
<tr>
<td>Recast</td>
<td>Apache 2.4.x &lt;2.4.25 Multiple Vulnerabilities</td>
<td>96401</td>
<td>High</td>
<td>Critical</td>
<td>All Assets</td>
<td>N/A</td>
<td>07/07/17</td>
<td><a href="mailto:screenshots@tenable.admin">screenshots@tenable.admin</a></td>
</tr>
<tr>
<td>Recast</td>
<td>CentOS 7 : openSSH (CVE-2016-2565)</td>
<td>83004</td>
<td>High</td>
<td>Critical</td>
<td>All Assets</td>
<td>N/A</td>
<td>07/07/17</td>
<td><a href="mailto:screenshots@tenable.admin">screenshots@tenable.admin</a></td>
</tr>
</tbody>
</table>

To delete one rule:

1. Click the ✗ button next to the rule you want to delete.

   Tenable.io deletes the rule. Tenable.io may take some time to remove the rule from existing vulnerabilities, depending on the system load and the number of matching vulnerabilities.

To delete multiple rules:

1. In the recast rules table, select the check box next to the each rule you want to delete.

2. Click **Delete**.
Tenable.io deletes the rules. Tenable.io may take some time to remove the rules from existing vulnerabilities, depending on the system load and the number of matching vulnerabilities.
Create an Accept Rule (Classic Interface)

**Required User Role:** Administrator

To create an accept rule:

1. In the top navigation bar, click **Settings**.
   
   The **About** page appears.

2. In the left navigation bar, click **Recast Rules**.
   
   The **Recast Rules** page appears.

3. Click **New Rule**.
   
   The **New Recast Rule** page appears.
4. In the **Target Vulnerability** box, type the ID of the plugin that you want to accept. For example, 51192.

   **Note:** If the plugin ID corresponds to a Nessus plugin, the **Original Severity** indicator changes to match the default severity of the vulnerability. The **Original Severity** indicator does not change if another type of plugin is used.

5. In the **Action** box, select **Accept**.

6. (Optional) If you want to report the vulnerability as a false positive, select the **Report as false positive** check box.

7. (Optional) In the **Comment** box, type a comment regarding the rule.
8. From the **Targets** drop-down box, do one of the following:

   - To target all assets, select **All**. This is the default target.
   - To target a custom set of assets:
      
      a. Select **Custom**.

      A **Target Hosts** box appears.

      b. In the **Target Hosts** box, type one or more targets for the rule.

      You can type a comma-delimited list that includes any combination of IP addresses, IP ranges, CIDR, and hostnames.

9. (Optional) In the **Expiration** box, set an expiration date for the rule. This action is only necessary if you want the rule to expire. By default, the rule applies indefinitely.

10. (Optional) In the **Comments** box, type a description of the rule. The text you type in this box is only visible if the rule is modified and has no functional effect.

11. Click **Save**.

    Tenable.io starts applying the rule to existing vulnerabilities. This process may take some time, depending on the system load and the number of matching vulnerabilities. The affected vulnerability is hidden on your workbench.

    **Note:** To view vulnerabilities hidden from your workbench, use the **Recast & Accept** advanced filter.
Delete an Accept Rule (Classic Interface)

**Required User Role:** Administrator

**Note:** When a rule is deleted or expires, the rule is reversed, and the change is reflected in the workbench.

To delete an accept rule:

1. In the top navigation bar, click **Settings**.
   
   The About page appears.

2. In the left navigation bar, click **Recast Rules**.
   
   The Recast Rules page appears.

   ![Recast Rules Table]

   Recast rules allow you to accept or modify the severity of a given vulnerability. In addition, rules can be limited to a specific asset or specific time frame. From this page you can view, create, edit, and delete your rules.

   To delete one rule:
   
   1. Click the ✗ button next to the rule you want to delete.

   Tenable.io deletes the rule. Tenable.io may take some time to remove the rules from existing vulnerabilities, depending on the system load and the number of matching vulnerabilities.

   To delete multiple rules:
   
   1. In the recast rules table, select the check box next to the each rule you want to delete.

   2. Click **Delete**.
Tenable.io deletes the rules. Tenable.io may take some time to remove the rule from existing vulnerabilities, depending on the system load and the number of matching vulnerabilities.
Edit an Accept Rule (Classic Interface)

**Required User Role:** Administrator

To edit an accept rule:

1. In the top navigation bar, click **Settings**.
   
   The **About** page appears.

2. In the left navigation bar, click **Recast Rules**.
   
   The **Recast Rules** page appears.

   ![Recast Rules Table]

   Recast rules allow you to accept or modify the severity of a given vulnerability. In addition, rules can be limited to a specific asset or specific time frame. From this page you can view, create, edit, and delete your rules.

<table>
<thead>
<tr>
<th>Action</th>
<th>Vulnerability</th>
<th>Plugin ID</th>
<th>Old Sev</th>
<th>New Sev</th>
<th>Targets</th>
<th>Expiration</th>
<th>Date Created</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>SSL Certificate Cannot Be Trusted</td>
<td>51192</td>
<td>Medium</td>
<td>N/A</td>
<td>All Assets</td>
<td>N/A</td>
<td>07/10/17</td>
<td><a href="mailto:screenname@tenable.admin">screenname@tenable.admin</a></td>
</tr>
<tr>
<td>Recast</td>
<td>SSH Weak Algorithms Supported</td>
<td>9517</td>
<td>Medium</td>
<td>Critical</td>
<td>172.16.48.104</td>
<td>N/A</td>
<td>07/07/17</td>
<td><a href="mailto:screenname@tenable.admin">screenname@tenable.admin</a></td>
</tr>
<tr>
<td>Recast</td>
<td>Apache 2.4.x &lt; 2.4.25 Multiple Vulnerability</td>
<td>6451</td>
<td>High</td>
<td>Critical</td>
<td>N/A</td>
<td>07/07/17</td>
<td><a href="mailto:screenname@tenable.admin">screenname@tenable.admin</a></td>
<td></td>
</tr>
<tr>
<td>Recast</td>
<td>CentOS 7: openssl (CVE-2016:2088)</td>
<td>6534</td>
<td>High</td>
<td>Critical</td>
<td>All Assets</td>
<td>N/A</td>
<td>07/07/17</td>
<td><a href="mailto:screenname@tenable.admin">screenname@tenable.admin</a></td>
</tr>
</tbody>
</table>

3. In the recast rules table, click the rule you want to edit.
   
   The **Edit Recast Rule** page appears.
4. Make any changes to the rule.

5. Click **Save**.

   Tenable.io saves the changes to the rule. Tenable.io may take some time to apply the changes to the rule and existing vulnerabilities, depending on the system load and the number of matching vulnerabilities.
You can add your own business context to assets by tagging them with descriptive metadata in Tenable.io. An asset tag is primarily composed of a Category:Value pair. For example, if you want to group your assets by location, create a Location category with the value Headquarters.

**Note:** If you want to create tags without individual categories, Tenable recommends that you add the generic category Category, which you can use for all your tags.

Adding your own business context to assets using tags allows you to configure scans to target assets with a specific tag, filter analysis views by tag, and assign assets to access groups.

**Note:** WAS widgets do not support tags at this time.

### Applying a Tag Manually vs. Automatically

You can apply a tag to assets *manually* or *automatically*.

- Manually applying a tag creates a static group of assets. You can create a tag and manually apply it to an asset later, or you can create a tag on-the-fly and manually apply it to an asset immediately.

  For example, to manually apply the Location:Headquarters tag to assets, create a tag without any tag rules. Then, you can manually apply the tag to assets located at your headquarters.

- Automatically applying a tag creates a dynamic group of assets, based on rules configured within the tag. You can create a tag with tag rules that Tenable.io then automatically applies to assets based on the tag rules.

  For example, to automatically apply the Location:Headquarters tag to assets within a specific IP address range, create a tag with a tag rule for that condition. Then, Tenable.io applies the tag based on asset attributes.

### Tag Management
Depending on your user role, you can view and search for tags via the Tags page. You can also search assets by tag via the Asset Details page.

For more information, see:

Examples: Asset Tagging
Tag Format and Application
View Tags
Create a Tag to Apply Manually
Create and Automatically Apply a Tag
Configure User Permissions for a Tag
Edit a Tag Category
Edit a Tag Value
Edit Tag Rules
Delete a Tag Category
Delete a Tag
Search for Assets by Tag from the Tags Table
Tags (Classic Interface)
Examples: Asset Tagging

See the following configuration examples to tag assets for common use cases. For general information about tags, see [Tags](#).

- [Example: Automatically Tag by Installed Software](#)
- [Example: Manually Tag by Priority](#)

**Example: Automatically Tag by Installed Software**

Your company manages assets that run on two software types: Oracle and Wireshark. Your company assigns asset ownership to employees based on the software type. Employees must resolve any vulnerabilities identified on assets with the software type they manage.

As an administrator, you can create an automatic tag for each software type. Then, employees can search for assets by the **Installed Software** tag and filter Tenable.io assets by the software type they manage.

**Note:** For more precise results, set the tag value to the appropriate NVD Common Platform Enumeration (CPE), for example, `cpe:/a:microsoft:office`.

To automatically tag assets by installed software:
1. **Create and automatically apply a tag** for Oracle assets using the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td><em>Installed Software</em></td>
</tr>
<tr>
<td>Value</td>
<td><em>Oracle</em></td>
</tr>
</tbody>
</table>
| Rules    | Enabled, with the following rule specified:  
  * Match All  
  * **Category**: *Installed Software*  
  * **Operator**: *is equal to*  
  * **Value**: *Oracle* |

2. **Create and automatically apply a tag** for Wireshark assets using the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td><em>Installed Software</em></td>
</tr>
<tr>
<td>Value</td>
<td><em>Wireshark</em></td>
</tr>
</tbody>
</table>
| Rules    | Enabled, with the following rule specified:  
  * Match All  
  * **Category**: *Installed Software*  
  * **Operator**: *is equal to*  
  * **Value**: *Wireshark* |

3. Instruct employees to use the new tags to [filter assets in the assets table](#) or to [search for assets from the tags table](#).  

**Example: Manually Tag by Priority**
Your company owns sensitive assets and you want employees to prioritize addressing vulnerabilities on these assets first, regardless of the asset's other attributes (for example, the asset's VPR).

To make sure employees view and mediate these sensitive assets first, you can create a High Priority tag and manually add it to assets that you want employees to prioritize. Then, employees can search for assets using the High Priority tag to filter by the highest priority assets they manage.

To manually tag assets by priority:

1. Create a tag for your highest priority assets using the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Priority</td>
</tr>
<tr>
<td>Value</td>
<td>High Priority</td>
</tr>
<tr>
<td>Value Description</td>
<td>A custom description about the urgency of remediating the vulnerabilities on assets with this tag.</td>
</tr>
</tbody>
</table>

2. Apply the tag manually to your highest priority assets.

3. Instruct employees to use the new tag to filter assets in the assets table or to search for assets from the tags table.
Tag Format and Application

An asset tag is primarily composed of a *Category:* *Value* pair. For example, if you want to group your assets by location, create a *Location* category with the value *Headquarters.*

**Note:** If you want to create tags without individual categories, Tenable recommends that you add the generic category *Category,* which you can use for all your tags.

You can apply a tag to assets either manually or automatically based on tag rules you specify. For example, if you want to apply the *Location:* *Headquarters* tag to assets within a specific IP address range, create a tag rule with that condition. Tenable.io then applies the tag based on asset attributes. Automatically applied tags are sometimes referred to as dynamic tags.

Tenable.io applies a dynamic tag when you add a new asset (via scan, connector import, or leveraging the Tenable.io API). When you update an existing asset, Tenable.io re-evaluates the asset and removes the tag if the asset's attributes no longer match the tag rules.

Tenable.io also re-evaluates tagged assets when you create or update tag rules.

**Note:** When you create or edit a tag rule, Tenable.io may take some time to apply the tag to existing assets, depending on the system load and the number of matching assets.

If you manually apply a tag that you've also configured with rules, Tenable.io excludes that asset from any further evaluation against the rules. To restore dynamic evaluations of the asset, remove the asset from the *Excluded Assets* list for that tag.

When configuring tag rules, you add rule criteria using most filters you would use to search for assets in the assets workbench. Supported filters include other tags. Unsupported filters include certain computed fields; for example, *Last Seen* and *Is Licensed.*

You can use the following icons to distinguish tags you've applied manually from automatically-applied tags:

<table>
<thead>
<tr>
<th>Location</th>
<th>Manual Application</th>
<th>Dynamic Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Detail page</td>
<td>🍀</td>
<td>🌟</td>
</tr>
</tbody>
</table>
View Tags

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

On the Tags page, you can view asset tag categories and tag values across Tenable.io. See Tags for more information about how tags can be used.

**Tip:** You can also search assets by tag via the Asset Details page.

To view tags:

1. In the upper-left corner, click the button.
   The left navigation plane appears.

2. In the left navigation plane, click Settings.
   The Settings page appears.

3. Click the Tagging tile.
   The Tags page appears. This page contains the Categories and Values tabs, which list asset tag categories and values.

View the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Categories, Values</td>
<td>The name of the tag.</td>
</tr>
<tr>
<td>Created By</td>
<td>Categories, Values</td>
<td>The username of the user who created the tag.</td>
</tr>
<tr>
<td>Last Used By</td>
<td>Categories, Values</td>
<td>The username of the user who most recently created or edited the tag value or tag category.</td>
</tr>
<tr>
<td>Created</td>
<td>Categories, Values</td>
<td>The date on which the tag was created.</td>
</tr>
<tr>
<td>Applied</td>
<td>Values</td>
<td>Indicates whether the tag is applied <strong>Manually or Automatically</strong>.</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td># of Assets</td>
<td>Values</td>
<td>The number of assets where the tag value is applied.</td>
</tr>
<tr>
<td># of Values</td>
<td>Categories</td>
<td>The number of tag values associated with the tag category.</td>
</tr>
</tbody>
</table>
Create a Tag to Apply Manually

**Required User Role:** Administrator

You can create a tag and manually apply it to assets. For more information, see [Tags](#).

To create a tag in the new interface:

1. In the upper-left corner, click the  button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Tagging** tile.
   
   The **Tags** page appears. This page contains the **Categories** and **Values** tabs, which list asset tag categories and values.

4. In the upper-right corner of the page, click the  create tag button.
   
   The **Create Tag** page appears.

5. Click the **Category** drop-down box.

6. In the **Add New Category** box, type a category.
   
   As you type, the list filters for matches.

7. From the drop-down box, select an existing category, or if the category is new, click **Create "category name"**.

   **Note:** You can create a maximum of 100 categories for your Tenable.io instance.

8. (Optional) In the **Category Description** box, type a description of the tag category.

9. In the **Value** box, type a tag value.
   
   For example, if the category is **Location**, type **Headquarters**. Tag values cannot include commas.
Note: Tag values cannot be more than 50 characters in length.

10. (Optional) In the **Value Description** box, type a description for the new tag value.

11. Click **Save**.

    Tenable.io creates the tag.

What to do next:

- Manually apply the tag to assets, as described in [Add a Tag to an Asset](#).
Create and Automatically Apply a Tag

**Required User Role:** Administrator

You can create a tag that Tenable.io automatically applies to assets using tag rules that you set. For more information, see [Tags](#) or [Considerations for Tags with Rules](#).

To create and automatically apply a tag in the new interface:

1. In the upper-left corner, click the button.
   
The left navigation plane appears.
2. In the left navigation plane, click **Settings**.
   
The **Settings** page appears.
3. Click the **Tagging** tile.
   
The **Tags** page appears. This page contains the **Categories** and **Values** tabs, which list asset tag categories and values.
4. In the upper-right corner of the page, click the **Create Tag** button.
   
The **Create Tag** page appears.
5. Click the **Category** drop-down box.
6. In the **Add New Category** box, type a category.
   
   As you type, the list filters for matches.
7. From the drop-down box, select an existing category, or if the category is new, click **Create "category name"**.

   **Note:** You can create a maximum of 100 categories for your Tenable.io instance.
8. (Optional) In the **Category Description** box, type a description of the tag category.
9. In the **Value** box, type a tag value.
For example, if the category is *Location*, type *Headquarters*. Tag values cannot include commas.

**Note:** Tag values cannot be more than 50 characters in length.

10. (Optional) In the **Value Description** box, type a description for the new tag value.

11. (Optional) Edit the list of assets excluded from the tag:

   a. In the **Excluded Assets** table, click the check box next to any previously-excluded asset that you now want to include in dynamic tag evaluations.

      The action bar appears at the bottom of the page.

   b. In the action bar, click the 🗓 button.

      A confirmation window appears.

   c. Click **Confirm**.

      Tenable.io re-evaluates the asset and applies the tag to the asset if the asset attributes match the tag's current rules.

12. Click **Save**.

    Tenable.io creates the tag. Tenable.io evaluates existing assets and automatically applies the tag to assets that match the tag rules.

    **Note:** When you create an automatic tag, Tenable.io may take some time to apply the rule to assets, depending on the system load and the number of assets.
Considerations for Tags with Rules

All users can create a tag to apply automatically to form a dynamic group of assets.

Automatic Application

Tenable.io evaluates assets against tag rules in the following situations:

- When you add a new asset (via scan, connector import, or leveraging the Tenable.io API), Tenable.io evaluates the asset against your tag rules.
- When you create or update a tag rule, Tenable.io evaluates your assets against the tag rule.

**Note:** When you create or edit a tag rule, Tenable.io may take some time to apply the tag to existing assets, depending on the system load and the number of matching assets.

- When you update an existing asset, Tenable.io re-evaluates the asset and removes the tag if the asset’s attributes no longer match the tag rules.

Manual Application

If you manually apply a tag that has been configured with rules, Tenable.io excludes that asset from any further evaluation against the rules.

To restore dynamic evaluations of the asset, remove the asset from the Excluded Assets list for that tag.
Configure User Permissions for a Tag

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

**Required Tag Permissions:** Creator

When creating a tag or editing a tag value, you can define the users or user groups that can edit the tag value. For more information, see Tags.

**Note:** When editing a tag value, if you are not the creator of the tag or an administrator, the Users & Groups section does not appear.

You can assign the following user or group permissions to a tag:

- **No Access** – *(All Users (Default) user group only)* No users (except for users or groups you specifically assign permissions) can edit the tag value.

- **Can Edit** – Users can edit the tag value. If you assign this permission to the *All Users (Default)* user group, all users can edit the tag value.

**Note:** The tag creator retains editing permissions, regardless of permissions changes made by other users.

To configure user permissions for a tag in the new interface:

1. Do one of the following:
   - Create a [manual](#) or [automatic](#) tag.
   - [Edit](#) a tag value.

2. In the **Users & Groups** section, do any of the following:
   - Edit permissions for the **All Users (Default)** user group.

   By default, the **All Users (Default)** user group permissions are set to **EditTag**. You can update this setting by doing the following:
- (Optional) From the permissions drop-down, select the permission you want to apply to the **All Users (Default)** group.

  Tenable adds a label representing the new permission to the user listing.

  - **Add permissions for any other user or user group.**
    - a. In the search box, type the name of a user or group.
      As you type, a filtered list of users and groups appears.
    - b. Select a user or group from the search results.
      Tenable.io adds the user to the **Users & Groups** section access group with the **EditTag** permission selected by default.
    - c. (Optional) From the permissions drop-down, select any permissions you want to apply to the user or user group.
      Tenable adds a label representing the new permission to the user listing.

  - **Remove permissions from a user or group.**
    - a. Locate the user or group you want to edit.
    - b. Roll over the label representing the permission you want to remove.
      The ✗ button appears on the label.
    - c. Click the ✗ button.

      Tenable.io removes the permission label from the user listing.

      If you remove the last permission for the **All Users (Default)** group, Tenable.io sets the group permissions to **No Access**.

  - **Remove a user or group from the tag.**
    - a. Roll over the user or group you want to delete.
    - b. Click the ✗ button next to the user or user group.

      The user or group disappears from the **Users & Groups** section.
3. Click **Save**.

Tenable.io creates the tag or updates the tag value.
Edit a Tag Category

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

When you edit a tag category, Tenable.io changes the category for all assets where that tag category is assigned.

To edit a tag category in the new interface:

1. In the upper-left corner, click the ☰️ button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Tagging** tile.
   
   The **Tags** page appears. This page contains the **Categories** and **Values** tabs, which list asset tag categories and values.

4. Click the **Categories** tab.
   
   The tag categories table appears.

5. In the tag categories table, click the category you want to edit.
   
   The **Edit Category** page appears.

6. In the **Category** box, edit the category.

7. (Optional) In the **Category Description** box, edit the description.

8. (Optional) Review or edit the values associated with the category:
   
   a. In the **Values** table, click the value you want to edit.
      
      The **Edit Tag** page appears.
   
   b. **Edit the tag value**.

9. Click **Save**.

   Tenable.io saves your changes and updates the tag.
Edit a Tag Value

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

When you edit a tag value, Tenable.io changes that value for all assets where that tag is assigned.

To edit a tag value:

1. In the upper-left corner, click the  button.
   
   The left navigation plane appears.
2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.
3. Click the **Tagging** tile.
   
   The **Tags** page appears. This page contains the **Categories** and **Values** tabs, which list asset tag categories and values.
4. Click the **Values** tab.
   
   The tags table appears.
5. In the tags table, click the tag you want to edit.
   
   The **Edit Tag** page appears.
6. In the **Value** box, edit the value.

   **Note:** Tag values cannot include commas.
7. (Optional) In the **Value Description** box, edit the description.
8. (Optional) Apply the tag based on rules:
   
   a. Click the **Rules** toggle to enable the tag rule settings.
      
      The tag rule settings appear.
   b. **Edit tag rules**.
9. (Optional) In the **Users & Groups** section, **Configure User Permissions for a Tag**.
10. **Click Save.**

   Tenable.io saves your changes and updates the tag.
Edit Tag Rules

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

When editing a tag to apply automatically, you add rules using most filters you would use to search for assets in the assets workbench. Supported filters also include other tags. Unsupported filters include certain computed fields; for example, **Last Seen** and **Is Licensed**.

**Note:** When you edit a tag rule, Tenable.io may take some time to apply the tag to existing assets, depending on the system load and the number of matching assets.

For more information about applying tags automatically, see [Tags](#) and [Considerations for Tags with Rules](#).

To edit tag rules in the new interface:

1. In the upper-left corner, click the **button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Tagging** tile.

   The **Tags** page appears. This page contains the **Categories** and **Values** tabs, which list asset tag categories and values.

4. Do one of the following:

   - To edit tag rules for a tag category, click the **Category** tab.
   - To edit tag rules for a tag value, click the **Value** tab.

5. In the tags table, click the tag you want to edit.

   The **Edit** page appears.

6. Edit the tag rules:
a. In the match drop-down box, do one of the following:
   - Click **Match All** to apply the tag only if an asset meets all of the tag rules you create.
   - Click **Match Any** to apply the tag if an asset matches any of the tag rules you create.

b. In the rule drop-down boxes, select an asset attribute and operator, then type a value for that attribute.
   
   For example, if you want to automatically apply this tag to all Windows assets, select **Operating System** and **contains**, then type *Windows*.

   **Note:** Not all attribute filters are supported when creating tag rules. For more information, see Asset Filters.

   **Note:** The value you specify for the attribute is not case sensitive. For example, if you type the hostname "hostx," the rule matches to assets with hostname "HOSTX" and "hostx."

c. (Optional) To add another tag rule, click the **Add** button.

   **Note:** You can add a maximum of 1,000 rules per individual tag.

d. (Optional) To see the number of assets that match your rules, click **Calculate affected assets**.

7. (Optional) Edit the saved search settings:

   **Note:** You must create a saved search before applying a tag using a saved search.

   a. Click the **Saved Search** toggle to enable the saved search settings.

   b. In the **Search** drop-down list, search for the saved search you want to apply to the tag.

      The list updates based on your search criteria.

      **Note:** You can only apply a tag to up to 5,000 assets at one time. If the **Saved Search** you select applies to more than 5,000 assets, you must edit the **Saved Search** or choose another one to apply to the tag.
8. (Optional) Edit the list of assets excluded from the tag:

   a. In the **Excluded Assets** table, click the check box next to any previously-excluded asset that you now want to include in dynamic tag evaluations.

      The action bar appears at the bottom of the page.

   b. In the action bar, click the button.

      A confirmation window appears.

   c. Click **Confirm**.

      Tenable.io re-evaluates the asset and applies the tag to the asset if the asset attributes match the tag’s current rules.

9. Click **Save**.

   Tenable.io updates the tag rules and applies the tag to matching assets.
Delete a Tag Category

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

When you delete a tag category, Tenable.io deletes any tags associated with that category and removes those tags from all assets where you applied them.

To delete a tag category in the new interface:

1. In the upper-left corner, click the button.  
   The left navigation plane appears.
2. In the left navigation plane, click **Settings**.  
   The **Settings** page appears.
3. Click the **Tagging** tile.  
   The **Tags** page appears. This page contains the **Categories** and **Values** tabs, which list asset tag categories and values.
4. Click the **Categories** tab.  
   The tag categories table appears.
5. To delete one tag category:
   a. In the tag category table, roll over the category you want to delete.  
      The action buttons appear in the row.
   b. Click the button.  
      A confirmation window appears.

To delete multiple tags:

a. In the tag category table, select the check box for each category you want to delete.  
   The action bar appears at the bottom of the page.

b. In the action bar, click the button.
A confirmation window appears.

6. Click **Confirm**.

Tenable.io deletes the tag category and any associated tags, and removes those tags from all assets where you applied them.
Delete a Tag

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

When you delete a tag, Tenable.io removes the tag from all assets where you applied the tag.

To delete one or more tags in the new interface:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, click Settings.
   
   The Settings page appears.

3. Click the Tagging tile.
   
   The Tags page appears. This page contains the Categories and Values tabs, which list asset tag categories and values.

4. Click the Values tab.

5. To delete one tag:
   
   a. In the tags table, roll over the tag you want to delete.
      
      The action buttons appear in the row.

   b. Click the button.
      
      A confirmation window appears.

To delete multiple tags:

a. In the tags table, select the check box for each tag you want to delete.
   
   The action bar appears at the bottom of the page.

b. In the action bar, click the button.
   
   A confirmation window appears.
6. Click **Confirm**.

Tenable.io deletes the tag and removes it from all assets where you applied the tag.
Search for Assets by Tag from the Tags Table

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

You can see what assets have a specific tag applied by searching for assets by tag.

To search for assets by tag from the tags table in the new interface:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Tagging** tile.
   
   The **Tags** page appears. This page contains the **Categories** and **Values** tabs, which list asset tag categories and values.

4. Click the **Values** tab.

5. In the table, roll over the tag you want search by.
   
   The action buttons appear in the row.

6. Click the button.
   
   The **Assets** page appears and displays the assets table filtered by the tag you selected.

**Note:** For more information on searching by assets from the assets table, see [Filter Assets by Tag](#).
Tags (Classic Interface)

Video: Categorizing Assets with Tags in Tenable.io

Add your own business context to assets by tagging them with descriptive metadata in Tenable.io.

You can manually apply a tag to create a static group of assets. You can also add rules to a tag to automatically apply the tag when the asset attributes match certain conditions, thereby creating a dynamic group of assets. For more information, see Tag Format and Application (Classic Interface).

You can create uniquely-named tags, which any user in your organization can apply to assets in Tenable.io, including Lumin. You can also provide descriptions of tags and tag categories to better explain their usage.

You can configure scans to target assets based on one or more tags you have assigned to the assets. You can also use applied tags to filter analysis views.

You can manage tags in any user role and view all the tags for your organization in a table on the Tags page. From the Tags page, you can perform the following tasks:

- Create a tag
- Edit a tag or tag category
- Edit tag rules
- Delete a tag
- Delete a tag category
- Search for assets by tag

Note: For information on applying or removing tags to assets, see Manage Asset Tags.
Tag Format and Application (Classic Interface)

An asset tag is primarily composed of a Category: Value pair. For example, if you want to group your assets by location, create a Location category with the value Headquarters.

Note: If you want to create tags without individual categories, Tenable recommends that you add the generic category Category, which you can use for all your tags.

You can apply a tag to assets either manually or automatically based on tag rules you specify. For example, if you want to apply the Location: Headquarters tag to assets within a specific IP address range, create a tag rule with that condition. Tenable.io then applies the tag based on asset attributes. Automatically applied tags are sometimes referred to as dynamic tags.

Tenable.io applies a dynamic tag when you add a new asset (via scan, connector import, or leveraging the Tenable.io API). When you update an existing asset, Tenable.io re-evaluates the asset and removes the tag if the asset's attributes no longer match the tag rules.

Tenable.io also re-evaluates tagged assets when you create or update tag rules.

Note: When you create or edit a tag rule, Tenable.io may take some time to apply the tag to existing assets, depending on the system load and the number of matching assets.

If you manually apply a tag that you've also configured with rules, Tenable.io excludes that asset from any further evaluation against the rules. To restore dynamic evaluations of the asset, remove the asset from the Excluded Assets list for that tag.

When configuring tag rules, you can use most filters you would use to search for assets in the assets workbench. Supported filters include other tags. Unsupported filters include certain computed fields; for example, Last Seen and Is Licensed.

You can use the following icons to distinguish tags you've applied manually from automatically-applied tags:

<table>
<thead>
<tr>
<th>Location</th>
<th>Manual Application</th>
<th>Dynamic Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tags column of the tags table (Settings &gt; Tags)</td>
<td>✏️</td>
<td>✏️</td>
</tr>
<tr>
<td>Tags section of the asset detail page (Dashboards &gt; Assets)</td>
<td>(no icon)</td>
<td>✝️</td>
</tr>
</tbody>
</table>
Create a Tag (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Note:** When you create a tag rule, Tenable.io may take some time to apply the tag to existing assets, depending on the system load and the number of matching assets.

To create an asset tag:

1. In the top navigation bar, click **Settings**.
   
The **About** page appears.

2. In the left navigation bar, click **Tags**.
   
The **Tags** page appears.

3. In the upper-right corner of the page, click the **Create Tag** button.
   
The **Create Tag** window appears.

4. **Configure a category:**
   
   **Add a new category:**

   In the **Category** box, type a name for the category.

   **Note:** You can create a maximum of 100 categories for your Tenable.io instance.

   **Use an existing category:**

   From the drop-down, select an existing category.

   **Note:** This field is required. If you want to create tags without individual categories, Tenable recommends that you add the generic category **Category**, which you can use for all your tags.

5. Type a tag value in the **Value** box. For example, if the category is **Location**, type **Headquarters**. Tag values cannot include commas.

6. (Optional) In the **Category Description** box, type a description of the tag category.

7. (Optional) In the **Value Description** box, type a description for the new tag value.
8. (Optional) Apply the tag automatically based on rules:
   a. Click **Apply automatically with rules** to expand the rule options.
   b. In the **Match** drop-down box, do one of the following:
      - Click **Any** to apply the tag if an asset matches any of the tag rules you create.
      - Click **All** to apply the tag only if an asset meets all of the tag rules you create.
   c. In the rule drop-down boxes, select an asset attribute and operator, then type a value for that attribute.
      
      For example, if you want to automatically tag any Windows assets, select **Operating System** and **contains**, then type **Windows**.
   d. (Optional) If you want to add another tag rule, click the + button next to the rule you created.

   **Note:** You can add a maximum of 1,000 rules per individual tag.

9. Click **Create**.
Edit a Tag or Tag Category (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

When you edit a tag, Tenable.io changes that value for all assets where that tag is assigned.

When you edit a tag category, Tenable.io changes that value for all assets where that tag category is assigned.

To edit a tag:

1. In the top navigation bar, click **Settings**.
   
   The **About** page appears.

2. In the left navigation bar, click **Tags**.

   The **Tags** page appears.

3. In the tags table, click the button next to the tag you want to edit.

4. Click **Edit Tag Value**. The **Edit Tag Value** window appears.

5. **Note:** Tag values cannot include commas.

6. (Optional) Edit the description in the second box.

7. (Optional) Apply the tag based on rules:
   
   a. Click **Apply automatically with rules**.
      
      The tag rule options appear.

   b. **Edit tag rules**.

8. Click **Save**.

   The **Confirm Changes** window appears.

9. Click **Save** to confirm changes.

To edit a tag category:
1. In the top navigation bar, click **Settings**.

   The About page appears.

2. In the left navigation bar, click **Tags**.

   The Tags page appears.

3. In the tags table, click the button next to any tag in the category you want to edit.

4. Click **Edit Tag Category**. The **Edit Tag Category** window appears.

5. Edit the value in the first box.

   **Note:** Tag values cannot include commas.

6. (Optional) Edit the description in the second box.

7. Click **Save**.

   The **Confirm Changes** window appears.

8. Click **Save** to confirm changes.
Edit Tag Rules (Classic Interface)

Required Tenable.io Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

Note: When you edit a tag rule, Tenable.io may take some time to apply the tag to existing assets, depending on the system load and the number of matching assets.

Note: You can add a maximum of 1,000 rules per individual tag.

To edit tag rules:

1. In the top navigation bar, click Settings.

   The About page appears.

2. In the left navigation bar, click Tags.

   The Tags page appears.

3. In the tags table, click the button next to the tag you want to edit.

4. Click Edit Tag Value.

   The Edit Tag Value window appears.

5. Do one of the following:

   - Edit the tag value or related descriptions.
   - In the Match drop-down box, click Any to apply the tag if an asset matches any of the tag rules you create, or click All to apply the tag only if an asset matches all of the tag rules you create.
   - In the rule drop-down boxes, select different attributes or operators for an existing rule.
   - Edit the rule value in the text box next to the rule drop-down boxes.

Note: The value you specify for the rule attribute is not case sensitive. For example, if you type the hostname "hostx," the rule matches to assets with hostname "HOSTX" and "hostx."
• Refine the list of assets excluded from the tag.
  a. In the **Excluded Assets** table, click the check box next to any previously-excluded asset or assets you now want to include in dynamic evaluations.
  b. Click **Remove Selected**.

  Tenable.io evaluates the asset and adds the tag to the asset if the asset attributes match the tag’s current rules.

• Add a new rule.
  a. Click the + button next to the last existing rule.
  b. In the rule drop-down boxes, select an asset attribute and operator.
  c. Type a value for the attribute.

6. Click **Save**.

   The **Confirm Changes** window appears.

7. Click **Save** to confirm.
Delete a Tag (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

When you delete a tag, Tenable.io removes the tag from all assets where you applied the tag.

To delete one or more tags:

**To delete one tag:**

1. In the top navigation bar, click **Settings**.
   
   The **About** page appears.

2. In the left navigation bar, click **Tags**.
   
   The **Tags** page appears.

3. In the tags table, click the button next to the tag you want to delete.

4. Click **Delete Tag Value**.
   
   The **Delete Tag** window appears.

5. Click **Delete** to confirm the deletion.

**To delete multiple tags:**

1. In the top navigation bar, click **Settings**.
   
   The **About** page appears.

2. In the left navigation bar, click **Tags**.
   
   The **Tags** page appears.

3. Select the check boxes next to the tags you want to delete.

4. Click the **Delete** button in the upper right corner of the page.
   
   The **Delete Tags** window appears.

5. Click **Delete** to confirm the deletion.
Delete a Tag Category (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

When you delete a tag category, the system deletes any tags associated with that category and removes those tags from all assets where you applied them.

**Tip:** You cannot delete multiple categories at the same time. Instead, delete each category individually.

To delete a tag category:

1. In the top navigation bar, click **Settings**.
   
   The About page appears.

2. In the left navigation bar, click **Tags**.
   
   The Tags page appears.

3. In the tags table, click the button next to any tag in the category you want to delete.

4. Click **Delete Tag Category**.
   
   The Delete Tag Category window appears.

5. Click **Delete** to confirm the deletion.
Search for Assets by Tag from the Tags Table (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

To search for assets by tag from the tags table:

1. In the top navigation bar, click **Settings**.
   
   The **About** page appears.

2. In the left navigation bar, click **Tags**.
   
   The **Tags** page appears.

3. In the tags table, click the button next to the tag by which you want to search.

4. In the drop-down box, click **Search Assets by Tag**.
   
   The **Assets** dashboard appears. The assets table is filtered by the tag you selected.

**Note:** For more information on searching by assets from the assets workbench, see [Filter Assets by Tag](#).
Managed Credentials

**Note:** This section describes creating and maintaining managed credentials. For more information about scan-specific or policy-specific credentials, see Credentials in Vulnerability Management Scans or Credentials in WAS Scans.

Managed credentials allow you to store credential settings centrally in a credential manager. You can then add those credential settings to multiple scan configurations instead of configuring credential settings for each individual scan.

You and users to whom you grant permissions can use managed credentials in scans. Credential user permissions control which users can use and edit managed credentials.

For information, see:
Create a Managed Credential

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

This topic describes creating a managed credential in the Tenable.io credential manager.

You can also create a managed credential during scan configuration, as well as convert a scan-specific credential to a managed credential. For more information, see Add a Credential to a Scan or Configure Credentials Settings in a Web Application Scan.

To create a managed credential:

1. In the upper-left corner, click the button.
   
The left navigation plane appears.

2. In the left navigation plane, click Settings.
   
The Settings page appears.

3. Click the Credentials tile.
   
The Credentials page appears. The credentials table lists the managed credentials you have permission to view.

4. In the upper-right corner of the page, click the Create Credential button.
   
The Select Credential Type plane appears.

5. Do one of the following:
   
   • Select one of the available credential types.
   
   • Click on a credential type in the category sections.

   The credential settings appear.

6. In the Title box, type a name for the credential.

7. (Optional) In the Description box, type a description for the credential.
8. Configure the settings for the credential type you selected.

   For more information about credential settings, see Credentials (Tenable.io) or Credentials (WAS).

9. Add user permissions.

10. Click Save.

    Tenable.io adds the credential to the credentials table in the Credentials page.
Edit a Managed Credential

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

This topic describes editing a credential in the Tenable.io credential manager.

You can also edit managed credentials during scan configuration. For more information, see [Add a Credential to a Scan](https://tenable.com/docs/managing/tenable.io/vulnerability-management/adding-a-credential-to-a-scan) for Tenable.io Vulnerability Management or [Configure Credentials Settings in a Web Application Scan](https://tenable.com/docs/managing/tenable.io/web-application-scanning/configuring-credentials-settings-in-a-web-application-scan) for Tenable.io Web Application Scanning.

You can edit any credentials where you have **Can Edit** permission.

To edit managed credentials:

1. In the upper-left corner, click the **️** button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Credentials** tile.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.

4. **Filter** or search the credentials table for the credential you want to edit. For more information, see [Tenable.io Tables](https://tenable.com/docs/managing/tenable.io/vulnerability-management/tenable.io-tables).

5. In the credentials table, click the name of the credential you want to edit.

   The credential settings plane appears.
6. Do one of the following:

   • **Edit the credential name or description.**
     
     a. Roll over the name or description box.
     
     b. Click the ✉ button that appears next to the box.
     
     c. Make your changes.
     
     d. Click the ✔ button at the lower right corner of the box to save your changes.

   • Edit the settings for the credential type. For more information about these settings, see [Credentials (Tenable.io)](https://tenable.io) or [Credentials (WAS)].
   
   • [Configure user permissions](https://tenable.io) for the credential.

7. Click **Save**.
Configure User Permissions for a Managed Credential

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

You configure user permissions for a managed credential separately from the permissions you configure for the scans where you use the credential.

You can configure credential permissions for individual users or a user group. If you configure credential permissions for a group, you assign all users in that group the same permissions. You may want to create the equivalent of a credential manager role by creating a group for the users you want to manage credentials. For more information, see [User Groups](#).

If you create a managed credential, Tenable.io automatically assigns you Can Edit permissions.

To configure user permissions for a managed credential:

1. Create or edit a managed credential:

<table>
<thead>
<tr>
<th>Location</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the credential manager</td>
<td>create or edit</td>
</tr>
<tr>
<td>In a scan configuration</td>
<td>create or edit</td>
</tr>
</tbody>
</table>

2. Do one of the following:

   - Add permissions for a user or user group.
     
     a. In the credential settings plane, click the button next to the User Permissions title.

     The Add User Permission settings appear.

     b. In the search box, type the name of a user or group.

     As you type, a filtered list of users and groups appears.

     c. Select a user or group from the search results.
d. Click the ▼ button next to the permission drop-down for the user or group.

e. Select a permission level:
   - **Can Use** – The user can view the credential in the managed credentials table and use the credential in scans.
   - **Can Edit** – The user can view and edit credential settings, delete the credential, and use the credential in scans.

f. Click Add.

g. Click Save.

• **Edit permissions for a user or user group.**
  a. In the **User Permissions** section of the credential settings plane, click the ▼ button next to the permission drop-down for the user or group.
  
  b. Select a permission level:
     - **Can Use** – The user can view the credential in the managed credentials table and use the credential in scans.
     - **Can Edit** – The user can view and edit credential settings, delete the credential, and use the credential in scans.
  
  c. Click Save.

• **Delete permissions for a user or user group.**
  a. In the **User Permissions** section of the credential settings plane, roll over the user or group you want to delete.
  
  b. Click the × button next to the user or user group.

    The user or group is removed from the **User Permissions** list.
  
  c. Click Save.
Delete a Managed Credential

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can delete any credentials where you have **Can Edit** permission.

To delete a managed credential:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Credentials** tile.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.

4. **Filter** or search the credentials table for the credential you want to delete. For more information, see [Tenable.io Tables](#).

5. In the table, roll over the credential you want to delete.

   The action buttons appear in the row.

6. Click the button.

   The **Confirm Deletion** window appears.

7. Do one of the following:

   - If no scans use the credential, click **Delete**.
   
   - If any scans use the credential:
a. Click **View Scans**.
   
   The **Scans** plane appears.

b. Filter or search for scans that use the credential.

c. Do one of the following:
   
   - Click **Cancel** to cancel the deletion.
   - Click **Delete** to confirm the deletion.
Access Groups

Note: System target group permissions that controlled viewing scan results and scanning specified targets have been migrated to access groups. For more information, see Scan Permissions Migration.

With access groups, you can control which users or groups in your organization can:

- View specific assets and related vulnerabilities in aggregated scan result views (dashboards in the new interface and workbenches in classic interface).
- Run scans against specific targets and view individual scan results for the targets.

An access group contains assets or targets as defined by the rules you set. Access group rules specify identifying attributes that Tenable.io uses to associate assets or targets with the group (for example, an AWS Account ID, FQDN, or IP address). By assigning permissions in the access group to users or user groups, you grant the users view or scan permissions for assets or targets associated with the access group.

Note: When you create or edit an access group, Tenable.io may take some time to assign assets to the access group, depending on the system load, the number of matching assets, and the number of vulnerabilities.

You can view the status of this assignment process in the Status column of the access groups table on the Access Groups page.

Only administrators can view, create, and edit access groups. As a user assigned any other role, you can see the access groups to which you belong and the related rules, but not the other users that are in the access group.

By default, all users have access to the All Assets group, which contains all assets. Therefore, if you want to limit permissions for assets, you must first restrict users for All Assets.

Note: Tenable.io applies dynamic tags to any assets, regardless of access group scoping. As a result, it may apply tags you create to assets outside of the access groups to which you belong.

Your organization can create up to 5,000 access groups.

For information on using access groups, see:
- Example: Access Groups
- Restrict Users for All Assets
- Create an Access Group
- Edit an Access Group
- Configure User Permissions for an Access Group
- View Assets Not Assigned to an Access Group
- View Your Assigned Access Groups
- Delete an Access Group
Example: Access Groups

In these examples, we walk through how an organization uses access groups to compartmentalize assets or targets into groups that reflect their organizational structure.

Note: These examples use the following format conventions:
- If the user group is Tenable-provided, the group name appears in bold (for example, All Users).
- If the user group is user-created, the group name appears in italics (for example, Atlanta Vuln Analysts).

Before you begin:
- Read the Access Groups topic to understand how access groups work.

Scenario 1 - Manage Assets

An organization wants to restrict which employees can see certain assets. This organization has locations in San Francisco and Atlanta. They want only the employees in Atlanta to view information for assets in the Atlanta office. Additionally, only the organization's administrators should be able to view all assets.

Step 1: Create user groups that reflect your organization's structure

The organization wants to easily assign permissions to multiple people at once, rather than each user individually. To do so, an administrator creates a user group and adds users. They create a user group that includes specific employees who work in the Atlanta office; for example, Atlanta Vuln Analysts. They also create a user group for employees who should have higher levels of access; for example, Administrators. Users can be a part of multiple user groups.

Step 2: Restrict user access to the All Assets access group

By default, All Users have both Can View and Can Scan access to the All Assets access group. The organization wants to use access groups to restrict what assets users can view and scan. Additionally, they only want the Administrators user group to have access to all assets. To ensure the All Assets access group does not override any other access group view restrictions, an administrator must first restrict user access to All Assets.

An administrator does the following in the All Assets access group:
• Assigns No Access permissions to the All Users user group.

• Assigns Can View permissions to the Administrators user group.

Users in the Administrators user group are able to view all assets, regardless of the access groups to which they are assigned. Everyone else in the organization is restricted from viewing all assets, and can only view assets in access groups they are assigned to.

Step 3: Create an access group

The organization has locations in San Francisco and Atlanta. They want to allow the employees in Atlanta to manage the assets in their office.

To do this, an administrator:

• Creates an access group called Atlanta Office. This access group must be the Manage Assets type of access group.

• Sets the Rules to filter assets in the Atlanta office into the Atlanta Office access group.

  Note: You can also create a rule based on an existing tag. For more information, see Tags.

• Retains the default No Access permissions for the All Users user group.

• Assigns Can View permissions to the Atlanta Vuln Analysts user group in the Atlanta Office access group. Only users in the Atlanta Vuln Analysts group can view scan results for assets in the Atlanta Office access group.

The organization now has an access group containing the organization’s Atlanta assets, to which only the Atlanta employees have access.

Scenario 2 - Scan Targets

In the Atlanta office, the organization wants to restrict which employees can configure and run scans against certain targets on the Atlanta office network. The organization wants the technical team leads to determine which scans other team members can run against targets in that network. The organization also wants the analysts in the Atlanta office to be able to view and analyze the results of the Atlanta network scans, but not configure or run the scans themselves.

Step 1: Create user groups that reflect your organization's structure
An administrator:

- Sets the **Role** for each user account.

<table>
<thead>
<tr>
<th>Employee</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atlanta team lead</td>
<td>Scan Manager</td>
</tr>
<tr>
<td>Atlanta team member</td>
<td>Scan Operator</td>
</tr>
<tr>
<td>Atlanta analyst</td>
<td>Basic</td>
</tr>
</tbody>
</table>

- **Creates** three user groups — *Atlanta Team Leads*, *Atlanta Team Members*, and *Atlanta Vuln Analysts*.

- **Adds** the employees to the appropriate user groups:

<table>
<thead>
<tr>
<th>Employee</th>
<th>User Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atlanta team lead</td>
<td>Atlanta Team Leads</td>
</tr>
<tr>
<td>Atlanta team member</td>
<td>Atlanta Team Members</td>
</tr>
<tr>
<td>Atlanta vulnerability analyst</td>
<td>Atlanta Vuln Analysts</td>
</tr>
</tbody>
</table>

**Step 2: Restrict user access to the All Assets access group**

By default, **All Users** have **Can View** and **Can Scan** access to the **All Assets** access group. The organization wants to use access groups to restrict what targets users can scan. Additionally, they only want the *Atlanta Vuln Analysts* user group to have view access to scan results for all targets in the access group. To ensure the **All Assets** access group does not override any other access group view restrictions, an administrator must first restrict user access to **All Assets**.

An administrator does the following in the **All Assets** access group:

- Assigns **No Access** permissions to the **All Users** user group.

- (Optional) To enable analysts to view all possible scan results without access group restriction, assigns **Can View** permissions to the *Atlanta Vuln Analysts* user group.

Users in the *Atlanta Vuln Analysts* user group are able to view scan results for all targets, regardless of which access groups they are assigned to. Everyone else in the organization is restricted from
viewing scan results for all targets, and can only view scan results for targets in access groups they are assigned to.

Step 3: Create an access group

An administrator:

- **Creates** a Scan Targets type of access group called **Atlanta Network**.
- Sets the **Rules** for the access group to match the IPv4 address range for the Atlanta office network, 192.0.2.0–192.0.2.255.
- **Assigns** the following permissions for user groups in the access group:

<table>
<thead>
<tr>
<th>User Group</th>
<th>Access Group Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Users</td>
<td>No Access</td>
</tr>
<tr>
<td>Atlanta Team Leads</td>
<td>Can View and Can Scan</td>
</tr>
<tr>
<td>Atlanta Team Members</td>
<td>Can View and Can Scan</td>
</tr>
<tr>
<td>Atlanta Vuln Analysts</td>
<td>Can View</td>
</tr>
</tbody>
</table>

**Note:** If the administrator configures Can View permissions for Atlanta Vuln Analysts in the All Assets access group, adding Can View permissions for Atlanta Vuln Analysts to the individual access group is not necessary.

Only users in the **Atlanta Team Leads**, **Atlanta Team Members**, and **Atlanta Vuln Analysts** groups have access to scan results for targets in this access group.

The organization now has an access group containing targets on the Atlanta network. Atlanta team leads and members can configure and run scans against targets in the access group. Atlanta team leads and members, as well as Atlanta vulnerability analysts, can view scan results for the targets in the access group.

Step 4: Configure a User-Defined Template
The lead for the Atlanta technical team configures a user-defined template called **Atlanta Network Template**. This user-defined template specifies parameters for the scans that team members can run.

**Step 5: Configure and Run a Scan**

A team member for the Atlanta technical team uses the **Atlanta Network Template** to configure a scan with a **Target** of 192.0.2.202 and schedules the scan to run daily. To make the scan results viewable, the team member must set the **Scan Results** option in the scan's **Basic settings** to **Show in dashboard**.

When it is time to run the scan, Tenable.io looks up the access groups to which the team member who configured the scan belongs, determines that **Atlanta Office Network** includes 192.0.2.202, then determines if the team member has adequate permissions:

- If the team member is assigned **Can Scan** permissions in the **Atlanta Office Network** access group, Tenable.io communicates the target to the scanner, which performs the scan and returns results.

- If the team member is **not** assigned **Can Scan** permissions in the **Atlanta Office Network** access group, Tenable.io does not communicate 192.0.2.202 as a target to the scanner. If this scan were configured for multiple targets, Tenable.io would communicate any other targets for which the team member has permissions, and the scanner would scan those targets. However, in this case, because there is a single target for the scan, the scan fails, and Tenable.io reports the scan status as aborted.

**Step 6: View Scan Results**

If the scan is successful, users in all three user groups (**Atlanta Team Leads**, **Atlanta Team Members**, and **Atlanta Vulns Analysts**) can view scan results in **individual scan views**, as well as in **vulnerabilities** tables, **assets** tables, and **dashboards**.
## Access Group Types

You can create the following types of access groups. Select an access group type based on the identifiers for the targets you want to scan.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Assets</td>
<td>Users can view the asset records created during previous scans and scan the associated targets for those assets. Use this type of access group if the targets you want to view and scan have been scanned before and can be best identified using tags based on asset attributes (for example, operating system or AWS Account ID).</td>
</tr>
<tr>
<td>Scan Targets</td>
<td>Users can scan targets associated with the access group and view the results of those scans. Use this type of access group if the targets you want to view and scan have never been scanned before and can only be identified using certain asset identifiers (specifically, FQDN, IPv4 address, or IPv6 address).</td>
</tr>
</tbody>
</table>

**Note:** The access group type names do not represent a limitation on the user actions that each group controls in relation to the specified targets. For both Manage Assets and Scan Targets groups, you can grant user permissions to view analytical results for the specified targets in dashboards, to scan the specified targets, or to both view and scan. For more information on user permissions, see Configure User Permissions for an Access Group.

**Tip:** You can add a user to both access group types if you want to allow the user to scan both types of scan targets.
Restrict Users for All Assets Group

**Required User Role:** Administrator

The **All Assets** group is the default, system-generated access group to which all assets belong.

By default, the following conditions are true:

- The **All Users** user group, which contains all users in your organization, is assigned to the **All Assets** access group.
- The permissions for the **All Users** group are set to **Can View** and **Can Scan**.

If you do not want all users to scan all assets and view the individual and aggregated results, you must set the permissions for the **All Users** group to **No Access**. Optionally, you can then add specific users or groups to provide individuals with access to all assets.

**Note:** When you create or edit an access group, Tenable.io may take some time to assign assets to the access group, depending on the system load, the number of matching assets, and the number of vulnerabilities.

You can view the status of this assignment process in the **Status** column of the access groups table on the **Access Groups** page.

To restrict user permissions for the **All Assets** group:

1. In the upper-left corner, click the **≡** button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Access Groups** tile.

   The **Access Groups** page appears. This page contains a table that lists the access groups to which you have access.

4. In the access groups table, click the **All Assets** group.

   The **Edit All Assets Access Group** page appears.
5. In the **Users & Groups** section, locate the listing for the **All Users** group.

6. Remove both the **Can Edit** and **Can Scan** labels from the **All Users** group listing:
   
a. Roll over the label.
   
The ⌇ button appears on the label.
   
b. Click the ⌇ button.
   
   Tenable.io removes the label.

   **Note:** When configuring permissions for the **All Users** user group, Tenable recommends keeping the following in mind:
   
   - If you retain the permissions for **All Assets** as **Can View**, all users can view scan results for all assets or targets for your organization.
   - If you set the permissions for **All Assets** to **Can Scan**, all users can scan all assets or targets for your organization and view the related scan results.

7. (Optional) **Configure** user permissions for each user or group you want to add to the **All Assets** group.

8. Click **Save**.

   The **Access Groups** page appears. Access to the **All Assets** group is restricted to the user(s) or group(s) you added.
Create an Access Group

**Required User Role:** Administrator

You can create an access group to group assets based on rules, using information such as an AWS Account ID, FQDN, IP address, and other identifying attributes. You can then assign permissions for users or user groups to view or scan the assets in the access group.

To create an access group:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Access Groups** tile.
   
   The **Access Groups** page appears. This page contains a table that lists the access groups to which you have access.

4. In the upper-right corner of the page, click the **Create Access Group** button.
   
   The **Create Access Group** page appears.

5. In the **General** section, in the **Name** box, type a name for the access group.

   **Note:** The name must be unique within your organization.

6. In the **Type** section, select the appropriate **access group type** based on the type of targets you want to scan.

   If you create an access group of one type, then change the type during configuration, Tenable.io prompts you to confirm the action. If you confirm, Tenable.io clears any previously added rule filters.

7. In the **Rules** section, add rules for the access group.
Access group rules specify the conditions Tenable.io evaluates when determining whether to include assets or targets in the access group.

**Note:** You can add up to 1,000 rules per access group.

a. In the **Category** drop-down box, select an attribute to filter assets or targets.

b. In the **Operator** drop-down box, select an operator.

Possible operators include:

- **is equal to:** Tenable.io matches the rule to assets or targets based on an exact match of the specified term.

  **Note:** Tenable.io interprets the operator as 'equals' for rules that specify a single IPv4 address, but interprets the operator as 'contains' for rules that specify an IPv4 range or CIDR range.

- **contains:** Tenable.io matches the rule to assets or targets based on a partial match of the specified term.

- **starts with:** Tenable.io matches the rule to assets or targets that start with the specified term.

- **ends with:** Tenable.io matches the rule to assets or targets that end with the specified term.

c. In the text box, type a valid value for the selected category.

  **Tip:** You can enter multiple values separated by commas. For **IPV4 Address**, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

d. (Optional) To add another rule, click the + **Add** button.

  **Note:** If you configure multiple rules for an access group, the access group includes assets or targets that match any of the rules. For example, if you configure two rules -- one that matches on the **Network Name** attribute and one that matches on **IPv4 Address**, the access group includes any assets in the specified network, plus any asset with the specified IPv4 address, regardless of whether that asset belongs to the specified network.

8. In the **Users & Groups** section, **configure** user permissions for the access group.
9. Click **Save**.

Tenable.io creates the access group. The **Access Groups** page appears.

**Note:** When you create or edit an access group, Tenable.io may take some time to assign assets to the access group, depending on the system load, the number of matching assets, and the number of vulnerabilities.

You can view the status of this assignment process in the **Status** column of the access groups table on the **Access Groups** page.
Configure User Permissions for an Access Group

**Required User Role:** Administrator

You can configure access group permissions for individual users or a user group. If you configure access group permissions for a group, you assign all users in that group the same permissions. For more information, see [User Groups](#).

You can assign the following access group permissions to a user or user group:

- **No Access** – (All Users user group only) No users (except for users or groups you specifically assign permissions) can scan the assets or targets specified in the access group. Also, no users can view related individual or aggregated scan results for the specified assets or targets.

- **Can View** – The user's view in aggregated scan results (workbenches/dashboards) includes data from scans of the assets or targets specified in the access group. If you assign this permission to the All Users group for the access group, all users can view aggregated scan results for the assets or targets in the access group.

- **Can Scan** – Users can scan assets or targets specified in the access group and view individual scan results for the assets or targets. If you do not have this permission, Tenable.io does not prevent you from configuring a scan using assets or targets specified in the access group; however, the scanner does not scan the assets or targets. If you assign this permission to the All Users group for the access group, all users can scan the assets or targets in the access group and view the related individual scan results.

User permissions in an access group are cumulative, rather than hierarchical. To allow a user to scan an asset or target and view results for that asset or target in aggregated results, you must set the user's permissions in the access group to both Can View and Can Scan.

**Tip:** To run scans auditing cloud infrastructure, configure a Scan Target access group that includes the target 127.0.0.1, and set user permissions to Can Scan.

To configure user permissions for an access group:

1. Create or edit an access group.

2. In the Users & Groups section, do any of the following:
• Edit permissions for the **All Users** user group.

The default values for the **All Users** user group depends on the access group:

• For the **All Assets** access group, Tenable.io assigns **Can View** and **Can Scan** permissions to the **All Users** group by default. Tenable recommends you restrict these permissions during initial configuration.

• For all other access groups, Tenable.io assigns **No Access** permissions to the **All Users** group by default. For these access groups, set permissions for the **All Users** group as follows:
  a. Next to the permission drop-down for the **All Users** group, click the » button.
  b. Click **Can View**.
  c. Next to the permission drop-down, click the » button again.
  d. Click **Can Scan**.
  e. Click **Save**.

    Tenable.io allows any user to view or scan the assets or targets in the group.

• Add a user to the access group.
  a. In the search box, type the name of a user or group.
     As you type, a filtered list of users and groups appears.
  b. Select a user or group from the search results.

    Tenable.io adds the user to the access group with the default **Can View** permissions and adds the related label to the user listing.

  c. (Optional) Add **Can Scan** permissions for the user.
     i. Next to the permission drop-down for the user or group, click the » button.
     ii. Click **Can Scan**.

      Tenable.io adds a **Can Scan** label to the user listing.
d. Click **Save**.

Tenable.io adds the user to the access group.

- **Add permissions for an existing user.**
  
  a. Locate the user or group you want to edit.
  
  b. Next to the permission drop-down for the user or group, click the ▼ button.
  
  c. Click **Can View** or **Can Scan** as appropriate.

      Tenable.io adds a label representing the new permission to the user listing.
  
  d. Click **Save**.

      Tenable.io saves your changes to the access group.

- **Remove permissions from an existing user.**
  
  a. Locate the user or group you want to edit.
  
  b. Roll over the label representing the permission you want to remove.

      The ✗ button appears on the label.
  
  c. Click the ✗ button.

      Tenable.io removes the permission label from the user listing.

      If you remove the last permission for the **All Users** group, Tenable.io sets the group permissions to **No Access**.

      If you remove the last permission for an individual user or group, Tenable.io prompts you to remove the user from the access group.

- **Remove a user from the access group.**
  
  a. Roll over the user or group you want to delete.
  
  b. Click the ✗ button next to the user or user group.

      The user or group disappears from the **Users & Groups** list.
c. Click **Save**.

Tenable.io saves your changes to the access group.
Edit an Access Group

**Required User Role:** Administrator

You can edit rules for an existing access group, as well as add or remove users and user groups assigned to the access group.

**Note:** You cannot edit the name or rules for the system-generated **All Assets** access group.

To edit an access group:

1. In the upper-left corner, click the ▪️ button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Access Groups** tile.
   
   The **Access Groups** page appears. This page contains a table that lists the access groups to which you have access.

4. In the access groups table, click the access group you want to edit.
   
   The **Edit Access Group** page appears.

5. In the **General** section, in the **Name** box, type a new name for the access group.

6. In the **Type** section, edit the access group type.
   
   a. Select the **access group type** to which you want to change.
      
      Tenable.io prompts you to confirm the action.

   b. Click **Confirm**.
      
      Tenable.io clears any previously added rule filters.

7. In the **Rules** section, edit the access group rules.
Access group rules specify the conditions Tenable.io evaluates when determining whether to include assets or targets in the access group.

- To edit an existing rule, modify the category, operator, and/or value as needed.
- To delete an existing rule, click the ✗ button next to the rule.
- To add a new rule, click ✦ Add and create a new rule.

8. In the **Users & Groups** section, configure user permissions for the access group.

9. Click **Save**.

Tenable.io updates the access group with your changes. The **Access Groups** page appears.

**Note:** When you create or edit an access group, Tenable.io may take some time to assign assets to the access group, depending on the system load, the number of matching assets, and the number of vulnerabilities.

You can view the status of this assignment process in the **Status** column of the access groups table on the **Access Groups** page.
View Assets Not Assigned to an Access Group

**Required User Role:** Administrator

If an asset does not match any access group rules, Tenable.io does not assign the asset to any access group. These unassigned assets are only visible to users in the **All Assets** group. If your organization limits membership in the **All Assets** group, users who are not members of the **All Assets** group are unable to see these unassigned assets, but this limited visibility may not be immediately obvious to them. If you are a member of the **All Assets** group, you can use a filter to identify these unassigned assets.

To view assets that are not assigned to an access group:

1. In the upper-left corner, click the **≡** button.
   
   The left navigation plane appears.

2. In the left navigation plane, in the **Asset View** section, click **Assets**.
   
   The **Assets** page appears.

3. **Create** a filter with the following settings:
   
   - **Category:** Belongs to Access Group
   - **Operator:** is equal to
   - **Value:** false

4. Click **Apply**.
   
   The assets table updates to display all assets that are not assigned to an access group.
View Your Assigned Access Groups

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

As an administrator, you can view the rules and assigned users and user groups for any access group. You can also edit access group parameters.

As a user in any other role, you can view your assigned access groups. This view includes the rules associated with each access group, but excludes the other users or user groups assigned to the access group. You cannot edit any access group settings.

To view your assigned access groups:

1. In the upper-left corner, click the ⬤ button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Access Groups** tile.
   
   The **Access Groups** page appears. This page contains a table that lists the access groups to which you have access.

4. (Optional) Click an access group to view more details.
   
   The **Edit Access Group** page appears.

   For administrators, this page contains both rules and assigned users and user groups, and you can edit all access group parameters.

   For users in any other role, this page contains rules only, and you cannot edit the rules.
Delete an Access Group

**Required User Role:** Administrator

**Note:** You cannot delete the system-generated *All Assets* group.

To delete one or more access groups:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Access Groups** tile.
   
   The **Access Groups** page appears. This page contains a table that lists the access groups to which you have access.

4. Select the access groups you want to delete:
   
   • **Select a single access group:**
     
     a. In the access groups table, roll over the access group you want to delete.
        
        The action buttons appear in the row.
     
     b. Click the button.
        
        A confirmation window appears.

   • **Select multiple access groups:**
     
     a. In the access groups table, select the check boxes next to the access groups you want to delete.
        
        The action bar appears at the bottom of the page.
b. In the action bar, click the button.

A confirmation window appears.

5. In the confirmation window, click the **Delete** button.

Tenable.io deletes the selected access group or groups and updates the access group table.
Access Group Rule Filters

You can use the filters described in the following sections to create rules for access groups. For more information, see:

- Tenable-provided Filters
- Guidelines for Tenable-provided Filters
- Tag Filters

Tenable-provided Filters

The last two columns in the following table indicate whether you can use the filter with the Manage Assets or Scan Targets group type.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
<th>Manage Assets</th>
<th>Scan Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Account ID</td>
<td>The canonical user identifier for the Amazon Web Services (AWS) account associated with the asset. For more information, see &quot;AWS Account Identifiers&quot; in the AWS documentation.</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>AWS Availability Zone</td>
<td>The name of the Availability Zone where AWS hosts the virtual machine instance. For more information, see &quot;Regions and Availability Zones&quot; in the AWS documentation.</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>AWS EC2 AMI ID</td>
<td>The unique identifier of the Linux AMI image in Amazon Elastic Compute Cloud (Amazon EC2). For more information, see the Amazon Elastic Compute Cloud Documentation.</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>AWS EC2 Instance ID</td>
<td>The unique identifier of the Linux</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Instance in Amazon EC2. For more information, see the Amazon Elastic Compute Cloud Documentation.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWS EC2 Name</td>
<td>The name of the virtual machine instance in Amazon EC2. yes</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>AWS EC2 Product Code</td>
<td>The product code associated with the AMI used to launch the virtual machine instance in Amazon EC2. yes</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>AWS Region</td>
<td>The region where AWS hosts the virtual machine instance, for example, 'us-east-1'. For more information, see &quot;Regions and Availability Zones&quot; in the AWS documentation. yes</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>AWS Security Group</td>
<td>The security group to which you have assigned the virtual machine instance in Amazon EC2. For more information, see Security Groups in the Amazon Virtual Private Cloud User Guide. yes</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>AWS Subnet ID</td>
<td>The unique identifier of the AWS subnet where the virtual machine instance was running at the time of the scan. yes</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>AWS VPC ID</td>
<td>The unique identifier of the public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private Cloud User Guide. yes</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>Azure Resource ID</td>
<td>The unique identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation. yes</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td><strong>Azure VM ID</strong></td>
<td>The unique identifier of the Microsoft Azure virtual machine instance. For more information, see &quot;Accessing and Using Azure VM Unique ID&quot; in the Microsoft Azure documentation.</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>
| **FQDN/Hostname** | One of the following:  
  - The fully-qualified domain name of the asset.  
  - The hostname of the asset. | yes | yes |
<p>| <strong>Google Cloud Instance ID</strong> | The unique identifier of the virtual machine instance in Google Cloud Platform (GCP). | yes | no |
| <strong>Google Cloud Project ID</strong> | The customized name of the project to which the virtual machine instance belongs in GCP. For more information, see &quot;Creating and Managing Projects&quot; in the GCP documentation. | yes | no |
| <strong>Google Cloud Zone</strong> | The zone where the virtual machine instance runs in GCP. For more information, see &quot;Regions and Zones&quot; in the GCP documentation. | yes | no |
| <strong>IPv4 Address</strong> | An IPv4 address for the asset. For this filter, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1). | yes | yes |
| <strong>IPv6 Address</strong> | An IPv6 address for the asset. | no | yes |
| <strong>MAC Address</strong> | The MAC address of the asset. | yes | no |</p>
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetBIOS Name</td>
<td>The NetBIOS name for the asset.</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Network Name</td>
<td>The name of the network to which the asset belongs.</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Operating System</td>
<td>The operating system installed on the asset.</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Qualys Asset ID</td>
<td>The Asset ID of the asset in Qualys. For more information, see the Qualys documentation.</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Qualys Host ID</td>
<td>The Host ID of the asset in Qualys. For more information, see the Qualys documentation.</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>ServiceNow Sys ID</td>
<td>The unique record identifier of the asset in ServiceNow. For more information, see the ServiceNow documentation.</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>

**Guidelines for Tenable-provided Filters**

- When configuring rules for **Scan Targets** access groups, the asset attribute type must match the target format used in the related scan. For example, if a **Scan Targets** access group rule filters on the FQDN/Hostname attribute, the related scan succeeds if the scan target is specified in FQDN or hostname format, but fails if the scan target is specified in IPv4 address format.

**Tag Filters**

In Tenable.io, tags allow you to add descriptive metadata to assets that helps you group assets by business context. For more information, see **Tags**.

You can use the tags you create to assign assets to **Manage Assets** access groups.

To add a tag filter to a rule:
1. In the **Category** drop-down box, select **Tags**.

2. In the **Operator** drop-down box, select **contains**.

3. In the text box, type the tag category and value you want to search for in the following format:

   Category Name:Value Name

4. Continue creating rules and/or save the access group as described in [Create an Access Group](#).

**Note:** Tag categories with 100,000 or more associated values cannot be applied as a rule to access groups.
# Scan Permissions Migration

System target group permissions that controlled whether users can scan specified targets have been migrated to access groups.

This migration affects your existing Tenable.io configuration as follows:

<table>
<thead>
<tr>
<th>Component</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing access group</td>
<td>Tenable.io:</td>
</tr>
<tr>
<td></td>
<td>• Updates any existing access group to an access group of the Manage Assets type.</td>
</tr>
<tr>
<td></td>
<td>• Replaces the All Users toggle with a default All Users group.</td>
</tr>
<tr>
<td></td>
<td>• Assigns Can View permissions to any existing users or user groups that currently have view access.</td>
</tr>
<tr>
<td>Existing system target groups</td>
<td>For each existing system target group, Tenable.io:</td>
</tr>
<tr>
<td></td>
<td>• Creates a new access group with a type of Scan Targets. This access group specifies the same scan targets as the existing system target group. Tenable.io lists migration as the owner of the migrated access groups.</td>
</tr>
<tr>
<td></td>
<td>• Moves any user with Can Scan permissions in the system target group to the new access group, and assigns the user Can Scan permissions for that access group. To ensure users can view results for the targets, configure Can View permissions for users in the access group.</td>
</tr>
</tbody>
</table>

**Note:** This migration does not delete existing system target groups. The migration removes only the Can Scan permissions from the system target groups.

**Note:** If, at the time of migration, an existing target group includes scan permissions, a Scan label may appear for the group in the Permissions column of the target groups table in the new Tenable.io user interface. This label indicates historical scan permissions only; access groups specify the current scan permissions.
| Existing scan configurations, dashboard filters, and saved searches | Existing scan configurations retain the system target group as a target setting. Existing dashboard filters and saved searches retain the system target group as a filter setting. If you have **Can Use** permissions for a system target group, you can continue to use the system target group to specify a group of targets in a scan configuration and to use the system target group in filters for dashboards and searches. However, to specify which users can view scan results for the targets, configure **Can View** permissions in the appropriate access group. |
My Account

**Note:** This section describes the new interface. For information about the classic interface, see [My Account (Classic Interface)](#). For information about navigating the new interface, see [Navigate Tenable.io (New Interface)](#).

From the **My Account** page, you can make changes to your own user account.

For more information, see the following topics:

- [Update Your Account](#)
- [Change a Password](#)
- [Configure Two-Factor Authentication](#)
- [Generate an API Key](#)
- [Unlock Your Account](#)
Update Your Account

**Required Tenable.io Vulnerability Management User Role**: Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role**: Basic, Scan Operator, Standard, Scan Manager, or Administrator

To update your account in the new interface:

1. Do one of the following:
   - In the upper-left corner, click the ☰ button.
     The left navigation plane appears.
     a. In the left navigation plane, click Settings.
        The Settings page appears.
     b. Click the My Account tile.
        The My Account page appears.
   - In the upper-right corner, click the ⚙ button.
     The user account menu appears.
     a. Click My Account.
        The My Account page appears.

2. (Optional) Edit your Name.

3. (Optional) Edit your Email.

   A valid email address must be in the format:

   ```
   name@domain
   ```

   where `domain` corresponds to a domain approved for your Tenable.io instance.
This email address overrides the email address set as your **Username**. If you leave this option empty, Tenable.io uses the **Username** value as your email address.

**Note:** During initial setup, Tenable configures approved domains for your Tenable.io instance. To add domains to your instance, contact Tenable Support.

4. Click **Save**.

   Tenable.io saves the changes to the account.

5. (Optional) **Change your password**.

6. (Optional) **Configure two-factor authentication**.

7. (Optional) **Generate an API key**.
Change Your Password

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can change the password for your own account as any type of user. The method of changing your password varies slightly based on the role assigned to your user account.

To change another user’s password, see Change Another User’s Password.

To change your password in the new interface:

1. Do one of the following:
   - In the upper-left corner, click the button.

   The left navigation plane appears.
   - In the left navigation plane, click Settings.

   The Settings page appears.
   - Click the My Account tile.

   The My Account page appears.
   - In the upper-right corner, click the button.

   The user account menu appears.
   - Click My Account.

   The My Account page appears.

2. In the Current Password box, type your current password.

3. In the New Password box, type a new password. See Password Requirements for more information.

4. Click the Save button.
Tenable.io saves the new password and terminates any currently active sessions for your account. Tenable.io then prompts you to re-authenticate.

5. **Log in** to Tenable.io using your new password.
Configure Two-Factor Authentication

Required Tenable.io Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Tenable.io Web Application Scanning User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can configure two-factor authentication for your account. Administrators cannot configure two-factor authentication for other users.

Note: Before configuring two-factor authentication, check the International Phone Availability list to ensure you are able to receive text messages from Tenable.io.

To add or modify two-factor authentication in the new interface:

1. Do one of the following:
   - In the upper-left corner, click the button.
     The left navigation plane appears.
     a. In the left navigation plane, click Settings.
        The Settings page appears.
     b. Click the My Account tile.
        The My Account page appears.
   - In the upper-right corner, click the button.
     The user account menu appears.
     a. Click My Account.
        The My Account page appears.

2. In the Enable Two Factor Authentication section, do one of the following:
• To enable SMS two factor authentication:
  
  a. Click **Enable SMS Two Factor Authentication**.

     The **Two-Factor Setup** plane appears.

  b. In the **Current Password** box, type your Tenable.io password.

  c. In the **Phone Number** box, type your mobile phone number.

     **Note:** By default, Tenable.io treats mobile numbers as U.S. numbers and prepends the +1 country code. If your mobile phone number is a non-U.S. number, be sure to prepend the appropriate country code.

  d. Click **Next**.

     The **Verification Code** plane appears and Tenable.io sends a text message with a verification code to the phone number.

  e. In the **Verification Code** box, type the verification code you received.

  f. Click **Next**.

     A **Two-Factor Setup Successful** message appears and Tenable.io applies your settings to your Tenable.io account.

  g. (Optional) To configure whether Tenable.io sends a verification code to the email associated with your user account:

     a. Select or clear the **Send backup email** check box.

     b. Click **Update**.

     Tenable.io updates your backup email settings.

• To enable authenticator application based authentication:
  
  a. Click **Enable Authenticator App**.

     The **Two-Factor Setup** plane appears.

  b. In the **Current Password** box, type your Tenable.io password.

  c. Click **Next**.
The **Time-based One-Time Password** plane appears.

d. In the authenticator application of your choice, scan the QR code.

In the authenticator application, a Tenable.io verification code appears.

e. In the **Verification Code** box, type the code provided by your authenticator application.

   **Note:** If you do not type the correct verification code, Tenable.io locks the QR code. Delete the setup from your authenticator application and scan a new QR code.

f. Click **Next**.

   A **Two-Factor Setup Successful** message appears and Tenable.io applies your settings to your Tenable.io account.

To disable two-factor authentication in the new interface:

1. Do one of the following:
   
   - In the upper-left corner, click the **≡** button.

   The left navigation plane appears.

   a. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

   b. Click the **My Account** tile.

   The **My Account** page appears.

   - In the upper-right corner, click the **👤** button.

   The user account menu appears.

   a. Click **My Account**.

   The **My Account** page appears.

2. In the **Change Password** section, in the **Current Password** box, type your current password.

3. In the **Enable Two Factor Authentication** section, click **Disable**.
A **Disable Two-Factor** confirmation message appears.

4. Read the warning message, then click **Continue**.

Tenable.io disables two-factor authentication for your account.
The API keys associated with your user account enable you to access the API for all Tenable.io products for which your organization is licensed.

**Note:** Tenable.io API access and secret keys are required to authenticate with the [Tenable.io API](https://www.tenable.io).

**Note:** The API keys associated with your user account enable you to access the API for all Tenable.io products for which your organization is licensed. You cannot set separate keys for individual products. For example, if you generate API keys in Tenable.io Vulnerability Management, this action also changes the API keys for Tenable.io Web Application Scanning and Tenable.io Container Security.

**Note:** Be sure to use one API key per application. Examples include, but are not limited to:

- Tenable.io integration
- Third-party integration
- Other custom applications, including those from Tenable Professional Services

The method to generate API keys varies depending on the role assigned to your user account. Administrators can generate API keys for any user account. For more information, see [Generate Another User's API Keys](https://www.tenable.io). Other roles can generate API keys for their own account.

To generate API keys for your own account in the new interface:

1. Do one of the following:
   
   - In the upper-left corner, click the **button.

     The left navigation plane appears.

     a. In the left navigation plane, click **Settings**.

     The **Settings** page appears.
b. Click the **My Account** tile.

The **My Account** page appears.

- In the upper-right corner, click the button.

The user account menu appears.

a. Click **My Account**.

The **My Account** page appears.

2. Click the **API Keys** tab.

The **API Keys** section appears.

3. Click **Generate**.

The **Generate API Keys** window appears with a warning.

**Caution:** Any existing API keys are replaced when you click the **Generate** button. You must update the applications where the previous API keys were used.

4. Review the warning and click **Generate**.

Tenable.io generates new access and secret keys, and displays the new keys in the **Custom API Keys** section of the page.

5. Copy the new access and secret keys to a safe location.

**Caution:** Be sure to copy the access and secret keys before you close the **API Keys** tab. After you close this tab, you cannot retrieve the keys from Tenable.io.
Unlock Your Account

Required Tenable.io Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Tenable.io Web Application Scanning User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Tenable.io locks you out if you attempt to log in and fail 5 consecutive times.

Note: If you no longer have access to the email address specified in your account, an administrator for your Tenable.io instance can reset your password instead.

To unlock your account:

1. On the Tenable.io login page, click the Forgot your password? link.
   The password reset page appears.

2. In the Username box, enter your Tenable.io username.

3. In the CAPTCHA box, type your answer to the question.

4. Click Send.
   Tenable.io sends password recovery instructions to the email address specified in your user account.

5. Reset your password using the instructions in the email message. See Password Requirements for more information.
My Account (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Note:** This topic describes the classic Tenable.io interface. For an introduction to the new interface, see [My Account](#) in the new interface.

To access the **My Account** page:

1. In the top navigation bar, click **Settings**.
   
   The **About** page appears.

2. In the left navigation bar, click **My Account**.

The **My Account** page appears. This page consists of the tabs described below.

**Account Settings**

On this tab, you can modify the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Info</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Full Name</strong></td>
<td>Your name.</td>
</tr>
</tbody>
</table>
| **Email** | Your email address.  

A valid email address must be in the following format:

*name@domain*

where *domain* corresponds to a domain approved for your Tenable.io instance.

This email address overrides the email address set as your **Username**. If you leave this option empty, Tenable.io uses the **Username** value as your email address.

**Note:** During initial setup, Tenable configures approved domains for your Tenable.io

---

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
To add domains to your instance, contact Tenable Support.

<table>
<thead>
<tr>
<th>Change Password</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Current Password</strong></td>
<td>Your current password. Required value when you <strong>change</strong> your password.</td>
</tr>
<tr>
<td><strong>New Password</strong></td>
<td>The new password you want to use. Enter a value to <strong>change</strong> your password.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Two-Factor</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable</strong></td>
<td><strong>Configure</strong> two-factor authentication for your account.</td>
</tr>
</tbody>
</table>

**API Keys**

On this tab, you can **generate** an API key.
**Users**

**Note:** This section describes the new interface. For information about the classic interface, see [Users (Classic Interface)](#). For information about navigating the new interface, see [Navigate Tenable.io (New Interface)](#).

User accounts provide access to Tenable.io and manage permissions for Tenable.io resources. Only administrators can create and manage user accounts.

**Note:** For an example of how user accounts interact with user groups and access groups in Tenable.io Vulnerability Management, see [Example: Access Groups](#).

To access the **Users** page, click **Settings** in the left navigation plane, then click the **Users** tile.

The **Users** page displays a table of all Tenable.io user accounts. This documentation refers to that table as the *users table*.

Each row of the users table includes the user name, the dates of the last login and last failed login attempt, the total number of failed attempts, and the role assigned to the account.

To control a user’s permissions in Tenable.io, you can assign [roles](#) to user accounts. You can change the role of a user account at any time.

You can also disable a user account to prevent a user from accessing Tenable.io. When you disable a user account, Tenable.io retains the user role previously assigned to that user, so the role is available when you enable the account again.

For more information about managing user accounts, see:

- [User Roles](#)
- [User Role Permissions](#)
- [Create a User Account](#)
- [Edit a User Account](#)
- [Change Another User’s Password](#)
- [Configure SSO Authentication](#)
- [Assist a User with Their Account](#)
- [Generate Another User’s API Keys](#)
• Unlock a User Account
• Disable a User Account
• Enable a User Account
• Manage User Access Authorizations
• Audit User Activity
• Delete a User Account
# User Roles

The following table briefly describes the available user roles and related permissions. For detailed permissions information, see [User Role Permissions](#).

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tenable.io Vulnerability Management User Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Basic</td>
<td>Can only manage their user profile and view scan results, including dashboards.</td>
</tr>
<tr>
<td>Scan Operator</td>
<td>Can create and run scans, but may only use existing scan user-defined scan templates that were created by a standard user or higher. They can create user target groups for use in scans.</td>
</tr>
<tr>
<td>Standard</td>
<td>In addition to scan operator privileges, can view user-defined scan templates that were created by a scan manager user or higher.</td>
</tr>
<tr>
<td>Scan Manager</td>
<td>In addition to standard user privileges, can configure scan settings and create, configure, use, and delete user-defined scan templates. They can also manage scanners, agents, and exclusions.</td>
</tr>
<tr>
<td>Administrator</td>
<td>Has all permissions, is responsible for setting up the account, and knows the organization's architecture. They can create groups to organize different business units, and add and manage users on the account.</td>
</tr>
<tr>
<td><strong>Tenable.io Web Application Scanning User Roles</strong></td>
<td></td>
</tr>
<tr>
<td>Basic</td>
<td>Can only manage their user profile and view scan results, including dashboards.</td>
</tr>
<tr>
<td>WAS Reader</td>
<td>Can only manage their user profile and view scan results, including dashboards.</td>
</tr>
<tr>
<td>WAS Scan Operator</td>
<td>Can create and run web application scans, but may only use existing scan user-defined scan templates that were created by a standard user or higher.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WAS Standard</td>
<td>In addition to scan operator privileges, can view user-defined scan templates that were created by a scan manager user or higher.</td>
</tr>
<tr>
<td>WAS Scan Manager</td>
<td>In addition to standard user privileges, can configure scan settings and create, configure, use, and delete user-defined scan templates.</td>
</tr>
<tr>
<td>Administrator</td>
<td>Has all permissions, is responsible for setting up the account, and knows the organization’s architecture. They can create groups to organize different business units, and add and manage users on the account.</td>
</tr>
</tbody>
</table>

**Tenable.io Container Security User Roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>Limited to viewing, searching, and filtering Tenable.io Container Security data.</td>
</tr>
<tr>
<td>Scan Operator and Standard</td>
<td>Can import, manage, and delete images and image repositories, but may only use policies set by a scan manager user or higher.</td>
</tr>
<tr>
<td>Scan Manager</td>
<td>In addition to scan operator privileges, can create, manage, and enforce policies.</td>
</tr>
<tr>
<td>Administrator</td>
<td>Has all permissions, is responsible for setting up the account, adding and managing users, and configuring connections to registries.</td>
</tr>
</tbody>
</table>
# User Role Permissions

**User roles** allow you to manage permissions for major functions in Tenable.io, controlling which Tenable.io resources users can access once logged in.

The following tables describe permissions by user role for major Tenable.io functions.

Each user role encompasses the permissions of lower roles and adds new permissions. Administrators have the most permissions, and basic users have the least.

<table>
<thead>
<tr>
<th>Area</th>
<th>Tenable.io Vulnerability Management User Roles and Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Administrator</td>
</tr>
<tr>
<td>API Keys</td>
<td>view, modify</td>
</tr>
<tr>
<td>About</td>
<td>view¹</td>
</tr>
<tr>
<td>Account Settings</td>
<td>view, modify</td>
</tr>
<tr>
<td>Access Groups</td>
<td>view, create, modify, delete</td>
</tr>
<tr>
<td>Agents</td>
<td>view, delete</td>
</tr>
<tr>
<td>Agent Blackout</td>
<td>view, create, modify, delete</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
</tr>
<tr>
<td>Agent Groups</td>
<td>view, create, modify, delete</td>
</tr>
</tbody>
</table>

¹Can view license information that is not available to other roles.
²Can view access groups they belong to and rules for those access groups. Cannot view other users who are members of those access groups.
<table>
<thead>
<tr>
<th>Area</th>
<th>Administrator</th>
<th>Scan Manager</th>
<th>Standard</th>
<th>Scan Operator</th>
<th>Basic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Settings</td>
<td>view, modify</td>
<td>view, modify</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Assets¹</td>
<td>view, modify, delete</td>
<td>view, modify, delete</td>
<td>view, modify, delete</td>
<td>view, modify, delete</td>
<td>view</td>
</tr>
<tr>
<td>Connectors</td>
<td>view, create, modify, delete</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Dashboards</td>
<td>view, create, modify, delete</td>
<td>view, create, modify, delete</td>
<td>view, create, modify, delete</td>
<td>view, create, modify, delete</td>
<td>view, create, modify, delete</td>
</tr>
<tr>
<td>Exclusions</td>
<td>view, import, export, delete</td>
<td>view, import, export, delete</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Health and Status</td>
<td>view</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Managed Credentials</td>
<td>view, create, modify, delete</td>
<td>view, create, modify, delete</td>
<td>view, create, modify, delete</td>
<td>view, create, modify, delete</td>
<td>view, create, modify, delete</td>
</tr>
<tr>
<td>PCI Managing</td>
<td>view, import,</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

¹Specific assets that a user can view are determined by access groups.
<table>
<thead>
<tr>
<th>Area</th>
<th>Tenable.io Vulnerability Management User Roles and Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Administrator</td>
</tr>
<tr>
<td></td>
<td>view, create, modify, delete</td>
</tr>
<tr>
<td>Recast Rules</td>
<td>view, create, modify, delete</td>
</tr>
<tr>
<td>Reports</td>
<td>view, run, create, modify, delete</td>
</tr>
<tr>
<td>Report Results</td>
<td>view, delete</td>
</tr>
<tr>
<td>Scans¹</td>
<td>view, import, run, create, modify, delete</td>
</tr>
<tr>
<td>Scan Results</td>
<td>view, delete</td>
</tr>
<tr>
<td>Sensors</td>
<td>view, add, modify, delete</td>
</tr>
</tbody>
</table>

¹User roles determine a user’s abilities, but the permissions that a user has for a particular scan are dictated by [scan permissions](#).

²Can create scans using existing user-defined policies that are shared with the user.

³Can view list of scans, but not scan configuration details.
## Tenable.io Vulnerability Management User Roles and Permissions

<table>
<thead>
<tr>
<th>Area</th>
<th>Administrator</th>
<th>Scan Manager</th>
<th>Standard</th>
<th>Scan Operator</th>
<th>Basic</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scanner Groups</strong></td>
<td>view, create, modify, delete</td>
<td>view, create, modify, delete</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>System Target Groups</strong></td>
<td>view, import, edit, modify, delete</td>
<td>view</td>
<td>view</td>
<td>view</td>
<td>-</td>
</tr>
<tr>
<td><strong>Tags</strong>¹</td>
<td>view, create tag category, create tag value, delete, assign, unassign</td>
<td>view, create tag value, delete, assign, unassign</td>
<td>view, delete, assign, unassign</td>
<td>view, delete, assign, unassign</td>
<td>view, assign, unassign</td>
</tr>
<tr>
<td><strong>User Groups</strong></td>
<td>view, create, modify, delete</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>User Target Groups</strong></td>
<td>view, import, export, create, modify, delete</td>
<td>view, import, create, export, modify, delete</td>
<td>view, import, create, export, modify, delete</td>
<td>view, import, create, export, modify, delete</td>
<td>-</td>
</tr>
<tr>
<td><strong>User-Defined Scan Templates</strong></td>
<td>view, import, export, create, modify, delete</td>
<td>view, import, export, create, modify,</td>
<td>view, import, export, create, modify,</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

¹Assigning and Unassigning tags can be done from the Asset Details page.
<table>
<thead>
<tr>
<th>Area</th>
<th>Administrator</th>
<th>Scan Manager</th>
<th>Standard</th>
<th>Scan Operator</th>
<th>Basic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>view, create, modify, delete</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>view, export</td>
<td>view, export</td>
<td>view, export</td>
<td>view, export</td>
<td>view, export</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Area</th>
<th>Administrator</th>
<th>Scan Manager</th>
<th>Standard</th>
<th>Scan Operator</th>
<th>Basic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboards</td>
<td>view, create, modify, delete</td>
<td>view, create, modify, delete</td>
<td>view, create, modify, delete</td>
<td>view, create, modify, delete</td>
<td>view</td>
</tr>
<tr>
<td>Tenable-Provided Scan Templates</td>
<td>view</td>
<td>view</td>
<td>view</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>User-Defined Scan Templates</td>
<td>view, create, modify, delete</td>
<td>view, create, modify, delete</td>
<td>view</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Scans (also requires scan permissions)</td>
<td>view, create, modify, run, delete</td>
<td>view, create, modify, run, delete</td>
<td>view, create, modify, run, delete</td>
<td>view, create(^1), modify, run, delete</td>
<td>view</td>
</tr>
</tbody>
</table>

^1 Can create scans using existing user-defined policies that are shared with the user.
## Tenable.io Web Application Scanning User Roles and Permissions

<table>
<thead>
<tr>
<th>Area</th>
<th>Administrator</th>
<th>Scan Manager</th>
<th>Standard</th>
<th>Scan Operator</th>
<th>Basic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed Credentials</td>
<td>view, create, modify, delete</td>
<td>view, create, modify, delete</td>
<td>view, create, modify, delete</td>
<td>view, create, modify, delete</td>
<td>view, create, modify, delete</td>
</tr>
<tr>
<td>Scan Permissions</td>
<td>view, create, modify, delete¹</td>
<td>view, create, modify, delete²</td>
<td>view, create, modify, delete³</td>
<td>view, create, modify, delete⁴</td>
<td>-</td>
</tr>
<tr>
<td>Scan Results (also requires scan permissions)</td>
<td>view, delete</td>
<td>view, delete</td>
<td>view, delete</td>
<td>view, delete</td>
<td>view, delete</td>
</tr>
</tbody>
</table>

## Tenable.io Container Security User Roles and Permissions

<table>
<thead>
<tr>
<th>Area</th>
<th>Administrator</th>
<th>Scan Manager</th>
<th>Standard</th>
<th>Scan Operator</th>
<th>Basic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboards</td>
<td>view</td>
<td>view</td>
<td>view</td>
<td>view</td>
<td>view</td>
</tr>
<tr>
<td>Usage Data</td>
<td>view⁵</td>
<td>view</td>
<td>view</td>
<td>view</td>
<td>view</td>
</tr>
<tr>
<td>Images</td>
<td>view, push to</td>
<td>view, push to</td>
<td>view, push</td>
<td>view, push</td>
<td>-</td>
</tr>
</tbody>
</table>

¹ Administrator users can create, modify, and delete permissions for scans that any user on the account owns.
² Scan Manager users can create, modify, or delete permissions only on scans they own.
³ Standard users can create, modify, or delete permissions only on scans they own.
⁴ Scan Operator users can create, modify, or delete permissions only on scans they own.
⁵ User with the Administrator role can view license information that is not available to other roles.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Tenable.io, delete</th>
<th>Tenable.io, delete</th>
<th>to Tenable.io, delete</th>
<th>to Tenable.io, delete</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Image Repository</strong></td>
<td>view, search, delete</td>
<td>view, search, delete</td>
<td>view, search, delete</td>
<td>view, search, delete</td>
</tr>
<tr>
<td><strong>Containers</strong></td>
<td>view</td>
<td>view</td>
<td>view</td>
<td>view</td>
</tr>
<tr>
<td><strong>Policies</strong></td>
<td>create, view, edit, set permissions, delete</td>
<td>create, view, edit, set permissions, delete</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Connectors</strong></td>
<td>create, configure, view, delete</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>CS Scanner</strong></td>
<td>download, view, configure, run</td>
<td>download, view, configure, run</td>
<td>download, view, configure, run</td>
<td>download, view, configure, run</td>
</tr>
<tr>
<td><strong>Scan Results</strong></td>
<td>view, search</td>
<td>view, search</td>
<td>view, search</td>
<td>view, search</td>
</tr>
<tr>
<td><strong>Connectors</strong></td>
<td>view, configure to import registries</td>
<td>view</td>
<td>view</td>
<td>view</td>
</tr>
</tbody>
</table>

1Besides user with the Administrator role, users can delete only images that they imported. Administrator users can delete images for all users on an account.
Tenable.io Password Requirements

Tenable.io enforces the following password requirements for all accounts:

Password Criteria

Passwords must be at least 12 characters long and contain the following:

- An uppercase letter
- A lowercase letter
- A number
- A special character

Password Expiration

Tenable.io passwords do not expire.

Account Lockout

By default, after 5 failed login attempts, Tenable.io locks the user out of their account. When a user is locked out of their account, they can unlock their own account, or an administrator can reset their password.

Password History

There are no limitations regarding password reuse.
Create a User Account

**Video:** Add a New User in Tenable.io

**Required User Role:** Administrator

To create a user account in the new interface:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Users** tile.

   The **Users** page appears. This page contains a table that lists all users for your Tenable.io instance.

4. In the upper-right corner of the page, click the **Create User** button.

   The **Create User** plane appears.

5. Configure the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Required</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Name</td>
<td>No</td>
<td>Type the first and last name of the user.</td>
</tr>
<tr>
<td>Username</td>
<td>Yes</td>
<td>Type a valid username.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A valid username must be in the format:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>\textit{name@domain}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>where \textit{domain} corresponds to a domain approved for your Tenable.io</td>
</tr>
</tbody>
</table>
| **Email** | **No** | Type a valid email address. A valid email address must be in the format:

\[
\text{name@domain}
\]

where \text{domain} corresponds to a domain approved for your Tenable.io instance.

This email address overrides the email address set in the **Username** box. If you leave this option empty, Tenable.io uses the **Username** value as the user's email address.

**Note:** During initial setup, Tenable configures approved domains for your Tenable.io instance. To add domains to your instance, contact your Tenable representative.

| **Password** | **Yes** | Type a valid password. See **Password Requirements** for more information.

In Tenable.io Web Application Scanning, passwords must be at least 12 characters long and contain the fol-
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>lowing:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• An uppercase letter</td>
<td>• A lowercase letter</td>
<td>• A number</td>
</tr>
<tr>
<td>• A special character</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| **Role** | **Yes** | **In the drop-down box, select the role that you want to assign to the user.** |

6. Click **Create**.

Tenable.io saves the account. The **Users** page appears, and the users table includes the new user account.
Edit a User Account

**Required User Role:** Administrator

To edit a user account in the new interface:

1. In the upper-left corner, click the `≡` button.
   - The left navigation plane appears.
2. In the left navigation plane, click **Settings**.
   - The **Settings** page appears.
3. Click the **Users** tile.
   - The **Users** page appears. This page contains a table that lists all users for your Tenable.io instance.
4. In the users table, click the name of the user that you want to edit.
   - The **Edit User** plane appears.
5. **Edit the name of the user.**
   a. At the top of the plane, click the name of the user.
      - A text box replaces the name.
   b. Type your changes.
   c. Click the `✓` button.
      - Tenable.io saves your changes.
6. **Configure the following options:**

<table>
<thead>
<tr>
<th>Option</th>
<th>Required</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Username</strong></td>
<td>-</td>
<td>You cannot edit this option.</td>
</tr>
<tr>
<td><strong>Email</strong></td>
<td>No</td>
<td>Type a valid email address.</td>
</tr>
</tbody>
</table>

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
A valid email address must be in the format:

\textit{name@domain}

where \textit{domain} corresponds to a domain approved for your Tenable.io instance.

This email address overrides the email address set in the \textbf{Username} box. If you leave this option empty, Tenable.io uses the \textbf{Username} value as the user's email address.

\begin{itemize}
  \item Note: During initial setup, Tenable configures approved domains for your Tenable.io instance. To add domains to your instance, contact your Tenable representative.
\end{itemize}

<table>
<thead>
<tr>
<th>New Password</th>
<th>Yes</th>
<th>Type a valid password. See Password Requirements for more information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>Yes</td>
<td>In the drop-down box, select the \textit{role} that you want to assign to the user.</td>
</tr>
</tbody>
</table>

7. Click \textbf{Save}.

Tenable.io saves the changes to the account.

8. (Optional) \textbf{Generate API keys} for the user.
Change Another User's Password

**Required User Role:** Administrator

To change the password for another user's account, you must be an administrator. To change your own password, see [Change Your Password](#).

To change another user's password in the new interface:

1. In the upper-left corner, click the button.
   
The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
The **Settings** page appears.

3. Click the **Users** tile.
   
The **Users** page appears. This page contains a table that lists all users for your Tenable.io instance.

4. In the users table, click the name of the user that you want to edit.
   
The **Edit User** plane appears.

5. In the **New Password** box, type a new password. See [Password Requirements](#) for more information.

6. Click **Save**.
   
   Tenable.io saves the new password for the user account.
Configure SSO/SAML Authentication

You can configure single sign-on (SSO)/Security Assertion Markup Language (SAML) authentication so users can use provider-initiated SSO when logging in to Tenable.io. By default, SSO is not enabled.

**Note:** Using SAML for your account does not disable traditional login.

Tenable.io supports:

- SAML 2.0-based authentication (for example, Okta or OneLogin)
- Shibboleth 1.3 authentication

**Note:** If you configure SSO authentication, Tenable.io does not log user actions to the audit log. This information may be available from the identity services provider you use.

**Note:** Tenable does not currently support a SP-Initiated SAML flow. Because it must be initiated from the Identity Provider side, navigating directly to https://cloud.tenable.com does not allow SSO. Additionally, all users must have an account configured in Tenable.io that matches their SSO login.

**Step 1: Configure SSO on the Tenable.io Side**

To configure SSO authentication:

1. Get the Identity Provider (IdP).xml metadata file from your SAML provider.

   **Note:** Follow your SAML providers instructions to generate the IdP .xml file.

2. Contact Tenable Support, provide the IdP .xml file and a valid Tenable.io email address, and ask Tenable Support to enable SAML on your account.

   Tenable Support uses the IdP .xml file you provided to generate the service provider (SP) .xml metadata file for you to finish configuring SSO.

   **Note:** If you are using ADFS or Azure AD as your IdP, the metadata may contain two (or more) signing certificates. Instead, follow the instructions in Configuring SAML Authentication with Tenable.io and Microsoft Azure AD.

**Step 2: Configure SSO on the SAML Side**
Note: These terms may vary between SSO providers.

To automatically configure SSO on the SAML side:
Upload the IdP .xml file you received from Tenable Support.

To manually configure SSO on the SAML side:
On the SAML side, configure the following parameters:

- **ACL/Single Sign On URL**: https://cloud.tenable.com/saml/login/<SAML_UUID>;
  
  Note: the SAML UUID can be obtained from the SP.xml provided by Tenable Support

- **NameID Format**: Unspecified

- **NameID Value**: The email address of the existing account in Tenable.io

- **Audience**: NessusCloud

Note: The following are the most common reasons that SAML configuration fails:

- The IDP metadata was generated incorrectly
- The IDP metadata included the incorrect certificate
- The SSO login does not match the Tenable.io login
Assist a User with Their Account

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Required User Role: Administrator

As an administrator, you can use the user assist functionality to simulate being logged in as another account. While assisting a user account, you can perform operations in Tenable.io as that user without needing to obtain their password or having to log out of your administrator account.

To assist a user with their account:

1. In the upper-left corner, click the ☐ button.

   The left navigation plane appears.

2. In the left navigation plane, click Settings.

   The Settings page appears.

3. Click the Users tile.

   The Users page appears. This page contains a table that lists all users for your Tenable.io instance.

4. In the users table, roll over the user account you want to assist.

   The action buttons appear in the row.

5. In the row, click the ☀ button.

   Tenable.io refreshes and displays the default dashboard for the user you are assisting. While you are assisting the user, Tenable.io displays an overlay at the top of each page with the role of the user you are assisting.

To stop assisting a user with their account:

- At the top of any page, in the overlay that displays the role of the user you are assisting, click the ✗ button.
Generate Another User's API Keys

**Required User Role:** Administrator

The API keys associated with your user account enable you to access the API for all Tenable.io products for which your organization is licensed. These keys must be used to authenticate with the Tenable.io REST API.

Administrators can generate API keys for any user account. Other roles can generate API keys for their own accounts. For more information, see [Generate API Keys](#).

**Note:** The API keys associated with your user account enable you to access the API for all Tenable.io products for which your organization is licensed. You cannot set separate keys for individual products. For example, if you generate API keys in Tenable.io Vulnerability Management, this action also changes the API keys for Tenable.io Web Application Scanning and Tenable.io Container Security.

To generate API keys for another user in the new interface:

1. [Edit a user account](#).
   
The Edit User plane appears.

2. In the **API Keys** section, click **Generate API Keys**.
   
   **Caution:** Any existing API keys are replaced when you generate new API keys. You must update the applications where the previous API keys were used.

   A warning message appears.

3. Review the warning and click **Replace & Generate**.
   
The new access and secret keys for the account appear in the plane.

4. Copy the new access and secret keys to a safe location.
   
   **Caution:** Be sure to copy the access and secret keys before you close the Edit User plane. After you close this plane, you cannot retrieve the keys from Tenable.io.
Unlock a User Account

Tenable.io locks you out if you attempt to log in and fail 5 consecutive times.

You can unlock a user account in one of the following ways:

- If a user has access to the email address specified in the user account, they can unlock their own account.
- If a user no longer has access to that email address, another user with administrator privileges can reset the user's password.
Disable a User Account

Required User Role: Administrator

Disabling a user account prevents the user from logging in and prevents their scans from running. You can enable a disabled user account as described in Enable a User Account.

To disable a user account in the new interface:

1. In the upper-left corner, click the button.
   The left navigation plane appears.

2. In the left navigation plane, click Settings.
   The Settings page appears.

3. Click the Users tile.
   The Users page appears. This page contains a table that lists all users for your Tenable.io instance.

4. Select the user or users you want to disable:
   - Select a single user:
     a. In the users table, roll over the user account you want to disable.
        The action buttons appear in the row.
     b. In the row, click the button.
        A confirmation window appears.
   - Select multiple users:
     a. In the users table, click the check box for each user you want to disable.
        The action bar appears at the bottom of the page.
     b. In the action bar, click the button.
        A confirmation window appears.
5. In the confirmation window, click **Disable**.

A success message appears.

Tenable.io disables the selected user or users. In the users table, a disabled user appears in light grey.

**Note:** If the user you disable has a session in progress, they may continue to have limited access. However, once they log out, they cannot log back in.
Enable a User Account

**Required User Role:** Administrator

If you **disable a user account**, you can enable an account again to restore a user's access.

To enable a user account in the new interface:

1. In the upper-left corner, click the  button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Users** tile.
   
   The **Users** page appears. This page contains a table that lists all users for your Tenable.io instance.

4. Select the user or users you want to enable:

   - **Select a single user:**
     
     a. In the users table, roll over the user account you want to enable.
        
        The action buttons appear in the row.

     b. In the row, click the ✓ button.
        
        A confirmation window appears.

   - **Select multiple users:**
     
     a. In the users table, click the check box for each user you want to enable.
        
        The action bar appears at the bottom of the page.

     b. In the action bar, click the ✓ button.
        
        A confirmation window appears.

5. In the confirmation window, click **Enable**.
A success message appears.

Tenable.io enables the selected user or users. In the users table, an enabled user appears in black.
Manage User Access Authorizations

Users can access Tenable.io using the following methods:

- Username and password login.
- Single sign-on (SSO). For more information, see Configure SSO/SAML Authentication.
- Tenable.io REST API with API keys. For more information, see Generate Another User's API Keys.

When you create a new user, all access methods are authorized by default. Depending on your organization's security policies, you may need to disable certain access methods, for example, disable username and password login to enforce SSO.

Use the Tenable.io Platform API to view, grant, and revoke access authorizations for a user. The following are examples of cURL commands to get a user's existing authorizations and then revoke the authorization for username and password login:

```
curl -H "X-APIKeys: accessKey=access_key;secretKey=secret_key" -X GET https://cloud.tenable.com/users/user_ID/authorizations
```

```
curl -H "X-APIKeys: accessKey=access_key;secretKey=secret_key" -d '{"api_permitted":true,"password_permitted":false,"saml_permitted":true}' -X PUT https://cloud.tenable.com/users/user_ID/authorizations
```

For more information, see Get User Authorizations and Update User Authorizations in the Tenable Developer Portal.
Audit User Activity

**Required User Role:** Administrator

In Tenable.io, the audit log records [user events](#) that take place in your organization's Tenable.io account. For each event, the log includes information about:

- the action taken
- the time at which the action was taken
- the user ID
- the target entity ID

The audit log provides visibility into the actions that users in your organization take in Tenable.io, and can be helpful for identifying security issues and other potential problems.

To view the audit log for your organization's Tenable.io account:

- Use the [Audit Log endpoint](#) as documented in the Tenable Developer Portal.

**Logged Events**

**Note:** If you configure SSO authentication for your users, Tenable.io does not write activity for those users to the audit log.

Audit log events include the following:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>audit.log.view</td>
<td>The system received and processed an audit-log request.</td>
</tr>
<tr>
<td>session.create</td>
<td>The system created a session for the user. This event can be triggered by</td>
</tr>
<tr>
<td></td>
<td>user login or authentication using an API key.</td>
</tr>
<tr>
<td>session.delete</td>
<td>The session expired, or the user ended a session.</td>
</tr>
<tr>
<td>session.impersonation.end</td>
<td>An administrator ended a session where they impersonated another user.</td>
</tr>
<tr>
<td>Event Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>session.impersonation.start</td>
<td>An administrator started a session where they impersonated another user.</td>
</tr>
<tr>
<td>user.authenticate.api-keys</td>
<td>The user authenticated a session start using an API key.</td>
</tr>
<tr>
<td>user.authenticate.mfa</td>
<td>Two-factor authentication was successful, and login was allowed.</td>
</tr>
<tr>
<td>user.authenticate.password</td>
<td>The user authenticated a session start using a password.</td>
</tr>
<tr>
<td>user.create</td>
<td>An administrator created a new user account.</td>
</tr>
<tr>
<td>user.delete</td>
<td>An administrator deleted a user account.</td>
</tr>
<tr>
<td>user.impersonation.end</td>
<td>An administrator stopped impersonating another user.</td>
</tr>
<tr>
<td>user.impersonation.start</td>
<td>An administrator started impersonating another user.</td>
</tr>
<tr>
<td>user.logout</td>
<td>The user logged out of their session.</td>
</tr>
<tr>
<td>user.update</td>
<td>Either an administrator or the user updated a user account.</td>
</tr>
</tbody>
</table>
Delete a User Account

**Required User Role:** Administrator

Before you delete a user account, you must first disable the user account.

**Caution:** Once you delete a user account, the account cannot be recovered and the action cannot be reversed.

The following table describes what objects are migrated, retained, or permanently deleted upon user deletion:

<table>
<thead>
<tr>
<th>Object Type</th>
<th>Deleted</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Schedules</td>
<td>No</td>
<td>Migrated to the new object owner</td>
</tr>
<tr>
<td>Historical Scan Results</td>
<td>No</td>
<td>Migrated to the new object owner</td>
</tr>
<tr>
<td>Scan Templates</td>
<td>No</td>
<td>Migrated to the new object owner</td>
</tr>
<tr>
<td>Custom Dashboards/Widgets</td>
<td>Yes</td>
<td>Permanently deleted</td>
</tr>
<tr>
<td>Managed Credentials</td>
<td>No</td>
<td>Retained (Created By value displays as null)</td>
</tr>
<tr>
<td>Tags</td>
<td>No</td>
<td>Retained (Created By value displays as null)</td>
</tr>
<tr>
<td>Recast/Accept Rules</td>
<td>No</td>
<td>Retained (Owner value displays as Unknown User)</td>
</tr>
<tr>
<td>Exclusions</td>
<td>No</td>
<td>Retained</td>
</tr>
<tr>
<td>System Target Groups</td>
<td>No</td>
<td>Retained</td>
</tr>
<tr>
<td>User Target Groups</td>
<td>Yes</td>
<td>Permanently deleted</td>
</tr>
<tr>
<td>Saved Searches</td>
<td>Yes</td>
<td>Permanently deleted</td>
</tr>
<tr>
<td>Connectors</td>
<td>No</td>
<td>Retained</td>
</tr>
<tr>
<td>Sensors</td>
<td>No</td>
<td>Retained</td>
</tr>
</tbody>
</table>

To delete a user account in the new interface:
1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Users** tile.

   The **Users** page appears. This page contains a table that lists all users for your Tenable.io instance.

4. In the users table, roll over the user account you want to delete.

   The action buttons appear in the row.

5. In the row, click the button.

   **Note:** If a user is not disabled, then the button does not appear. **Disable** the user before deleting them.

   **Note:** You cannot delete the **Default Administrator** account. If you want to delete the Default Administra- tor account, you must contact Tenable Support.

   The **Delete User** page appears.

6. In the **Transfer User Objects** section, from the **Select New Object Owner** drop-down box, select the user to which you want to transfer any of the user's objects (e.g., scan results, user-defined scan templates).

7. Click **Delete**.

   A confirmation message appears.

8. Click **Delete**.

   Tenable.io deletes the user and transfers any user objects to the user you designated.
Users (Classic Interface)

**Note:** This section describes the classic Tenable.io interface. For an introduction to the new interface, see Users in the new interface.

User accounts enable you to provide access to Tenable.io and manage permissions for Tenable.io resources. Only administrators can create and manage user accounts.

To access the Users page, click Settings in the top navigation bar, then click Users in the left navigation bar.

The Users page displays a table of all Tenable.io user accounts. This documentation refers to that table as the users table.

Each row of the users table includes the user name, the dates of the last login and last failed login attempt, the total number of failed attempts, and the role assigned to the account.

To control a user's permissions in Tenable.io, you can assign roles to user accounts. You can change the role of a user account at any time.

You can disable a user account to prevent a user from accessing Tenable.io. When you disable a user account, Tenable.io retains the user role assigned to that user.

You can change the role of a user account at any time, as well as disable the account.

Via the Users page, you can:

- [Create a User Account (Classic Interface)]
- [Edit a User Account (Classic Interface)]
- [Generate API Keys (Classic Interface)]
- [Impersonate a User Account (Classic Interface)]
- [Disable a User Account (Classic Interface)]
- [Enable a User Account (Classic Interface)]
- [Delete a User Account]
Create a User Account (Classic Interface)

**Required User Role:** Administrator

To create a user account:

1. In the top navigation bar, click **Settings**.
   
   The **About** page appears.

2. In the left navigation bar, click **Users**.
   
   The **Users** page appears.

3. In the upper-right corner of the page, click **New User**.
   
   The **New User** page appears.

4. Configure the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Required</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Yes</td>
<td>Type a valid username. A valid username must be in the format: <code>name@domain</code> where <code>domain</code> corresponds to a domain approved for your Tenable.io instance. <strong>Note:</strong> During initial setup, Tenable configures approved domains for your Tenable.io instance. To add domains to your instance, contact your Tenable representative.</td>
</tr>
<tr>
<td>Full Name</td>
<td>No</td>
<td>Type the full name of the user.</td>
</tr>
<tr>
<td>Email</td>
<td>No</td>
<td>Type a valid email address. A valid email address must be in the format: <code>name@domain</code></td>
</tr>
</tbody>
</table>
where \textit{domain} corresponds to a domain approved for your Tenable.io instance.

This email address overrides the email address set in the \textbf{Username} box. If you leave this option empty, Tenable.io uses the \textbf{Username} value as the user's email address.

\textbf{Note:} During initial setup, Tenable configures approved domains for your Tenable.io instance. To add domains to your instance, contact your Tenable representative.

<table>
<thead>
<tr>
<th>Password</th>
<th>Yes</th>
<th>Type a valid password. See \textbf{Password Requirements} for more information.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>In Tenable.io Web Application Scanning, passwords must be at least 12 characters long and contain the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• An uppercase letter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A lowercase letter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A special character</td>
</tr>
</tbody>
</table>

| Role     | Yes | In the drop-down box, select the \textit{role} that you want to assign to the user. |

5. Click \textbf{Save}.

Tenable.io saves the account. The \textbf{Accounts} page appears, where you can view the new user account.
**Edit a User Account (Classic Interface)**

**Required User Role:** Administrator

To edit a user account:

1. In the top navigation bar, click *Settings*.
   
   The *About* page appears.

2. In the left navigation bar, click *Users*.
   
   The *Users* page appears.

3. In the users table, click the name of the user that you want to edit.
   
   The *Edit User* page appears.

4. Configure the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Required</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Enabled</td>
<td>No</td>
<td>Enable or disable the account.</td>
</tr>
<tr>
<td>Full Name</td>
<td>No</td>
<td>Type the full name of the user.</td>
</tr>
<tr>
<td>Email</td>
<td>No</td>
<td>Type a valid email address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A valid email address must be in the format:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>name@domain</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>where <em>domain</em> corresponds to a domain approved for your Tenable.io instance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This email address overrides the email address set in the <em>Username</em> box. If you leave this option empty, Tenable.io uses the <em>Username</em> value as the user's email address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: During initial setup, Tenable configures approved domains for your Tenable.io instance. To add domains to your instance, contact your Tenable representative.</td>
</tr>
<tr>
<td>----------------</td>
<td>---</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Yes</td>
<td>Change the password for the account.</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>Yes</td>
<td>In the drop-down box, select the role that you want to assign to the user.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

   Tenable.io saves the changes to the account.

6. (Optional) **Generate API keys** for the account.
Configure Two-Factor Authentication (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can configure two-factor authentication for your account. Administrators cannot configure two-factor authentication for other users.

**Note:** Before configuring two-factor authentication, check the [International Phone Availability] list to ensure you are able to receive text messages from Tenable.io.

To configure two-factor authentication in the classic interface:

**To add or modify two-factor authentication:**

1. In the top navigation bar, click **Settings**.
   
   The **About** page appears.

2. In the left navigation bar, click **My Account**.
   
   The **My Account** page appears.

3. In the **Two-Factor** section:
   
   - If enabling two-factor authentication for the first time, click **Enable**.
   - If modifying an existing configuration, click **Edit**.

   The **Two-Factor Setup** box appears.

4. Type your mobile phone number in the box.

   **Note:** By default, Tenable.io treats mobile numbers as U.S. numbers and prepends the +1 country code. If your mobile phone number is a non-U.S. number, be sure to prepend the appropriate country code.

5. Click **Next**.

   The **Verification Code** screen appears and Tenable.io sends a text message with a verification code to the phone number.

6. Type the verification code in the box.
7. Click **Next**.

The **Success** screen appears.

8. Click **Close**.

9. (Optional) Select the **Send backup email** check box if you want Tenable.io to send a verification code to the email associated with your user account.

10. (Optional) To return to the new interface, in the top navigation bar, click **New Interface**.

**To disable two-factor authentication:**

1. In the top navigation bar, click **Settings**.

   The **About** page appears.

2. In the left navigation bar, click **My Account**.

   The **My Account** page appears.

3. In the **Two-Factor** section, click **Disable**.

   The **Disable Two-Factor** window appears and a warning message indicates that if you disable this feature for the account, Tenable.io deletes the mobile phone number and other settings associated with the feature.

4. Click **Continue**.

5. (Optional) To return to the new interface, in the top navigation bar, click **New Interface**.
Change a Password (Classic Interface)

You can change the password for your account as any type of user. To change the password for another user's account, you must be an administrator.

The method of changing your password varies slightly based on the role assigned to your user account.

To change a password:

1. Do one of the following:

   As an administrator:
   1. [Edit a user account](#).
      
      The **Edit User** page appears.
   
   As a standard or basic user:
   
   a. In the top navigation bar, click **Settings**.
      
      The **About** page appears.
   
   b. In the left navigation bar, click **My Account**.
      
      The **My Account** page appears.

2. Type your current password in the **Current Password** box.

3. In the **New Password** box, type a new password.

   **Note:** Passwords must be at least 12 characters long and contain the following:
   
   - An uppercase letter
   - A lowercase letter
   - A number
   - A special character

4. Click the **Save** button.
Tenable.io saves the new password. Tenable.io terminates any currently active sessions for the modified account.

If you changed your own password, Tenable.io prompts you to re-authenticate.

If you changed a password for another user, Tenable.io prompts the user to re-authenticate.

5. [Log in](#) to Tenable.io using the new password.
Generate API Keys (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

The API keys associated with your user account enable you to access the API for all Tenable.io products for which your organization is licensed.

**Note:** Tenable.io API access and secret keys are required to use the Tenable.io API.

**Note:** The API keys associated with your user account enable you to access the API for all Tenable.io products for which your organization is licensed. You cannot set separate keys for individual products. For example, if you generate API keys in Tenable.io Vulnerability Management, this action also changes the API keys for Tenable.io Web Application Scanning and Tenable.io Container Security.

You can perform this procedure as any user. However, the method to generate API keys varies depending on the role assigned to your user account. Administrators can generate API keys for any user account.

To generate API keys:

1. Do one of the following:
   
   **As an administrator:**
   
   1. [Edit a user account](#).

      The Edit User page appears.

   **As a standard or basic user:**
   
   1. In the upper-right corner of the top navigation bar, click your name.

   2. Click [My Account](#).

      The My Account page appears.

2. In the center pane, click the API Keys tab.

   The API Keys section appears.

3. Click Generate.
**Caution:** Any existing API keys are replaced when you click the Generate button. You must update the applications where the previous API keys were used.

Tenable.io generates access and secret keys for your account. These keys must be used to authenticate with the Tenable.io REST API.

**Caution:** After you generate your API key, copy and save the key to a safe location. Without saving the keys, you cannot retrieve the keys from Tenable.io.
Impersonate a User Account (Classic Interface)

**Required User Role:** Administrator

As an administrator, you can impersonate all other user accounts. While impersonating an account, you can perform operations in Tenable.io as another user without needing to obtain that user’s password, or having to log out of your administrator account in order to log in as another user.

To impersonate a user account:

1. In the top navigation bar, click **Settings**.
   
   The **About** page appears.

2. In the left navigation bar, click **Users**.
   
   The **Users** page appears.

3. In the users table, click the username of the user that you want to impersonate.
   
   The **Edit User** page appears.

4. In the upper-right corner, click **Impersonate**.
   
   You start impersonating the user. The user’s default dashboard appears, and the user’s name appears in the upper-right corner of the top navigation bar.

To stop impersonating a user account:

1. In the upper-right corner of the top navigation bar, click the username of the account you are impersonating.

2. Click **Leave User**.

   You stop impersonating the user. The **Edit User** page for the user appears, and your username appears in the upper-right corner of the top navigation bar.
Disable a User Account (Classic Interface)

**Required User Role:** Administrator

Disabling a user account prevents the user from logging in and prevents their scans from running. You can enable a disabled user account as described in [Enable a User Account (Classic Interface)](#).

To disable a user account:

1. In the top navigation bar, click **Settings**.
   
   The **About** page appears.

2. In the left navigation bar, click **Users**.
   
   The **Users** page appears.

3. In the users table, click the check box next to the user account you want to disable.
   
   The **Disable** button appears at the top of the screen.

4. Click the **Disable** button.
   
   The **Disable User** window appears.

5. Click **Continue**.
   
   A success message appears.

   Tenable.io disables the user account and tags it as **Disabled** in the users table.

**Note:** If the user being disabled has a session in progress, they may continue to have limited access. However, once they log out, they cannot log back in.
Enable a User Account (Classic Interface)

Required User Role: Administrator

If you disable a user account, you can enable an account again to restore a user's access.

To enable a user account in the classic interface:

1. In the top navigation bar, click Settings.
   The About page appears.
2. In the left navigation bar, click Users.
   The Users page appears.
3. In the users table, click the check box next to the disabled user account you want to enable.
   The Enable button appears at the top of the screen.
4. Click the Enable button.
   The Enable User window appears.
5. Click Continue.
   A success message appears.
   Tenable.io enables the user account.
User Groups

**Note:** This section describes the new interface. For information about the classic interface, see Groups (Classic Interface). For information about navigating the new interface, see Navigate Tenable.io (New Interface).

**Note:** For an example of how user groups interact with user accounts and access groups, see Example: Access Groups.

To access the **User Groups** page, click **Settings** in the left navigation plane, then click the **Groups** tile.

The **User Groups** page displays a table of all user groups in your Tenable.io instance. This documentation refers to that table as the **user groups table**.

You can assign groups permissions for scans, user-defined scan templates, access groups, target groups, and agents. When you assign users to a group, the users inherit the permissions assigned to the group. Your organization may utilize groups to provide permissions to batches of users based on the roles of those users and your organization's security posture.

To manage user groups, see the following:

- [Create a Group](#)
- [Edit a Group](#)
- [Delete a Group](#)
Create a User Group

Required User Role: Administrator

To create a user group:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, click Settings.

   The Settings page appears.

3. Click the Groups tile.

   The User Groups page appears. This page contains a table that lists all user groups for your Tenable.io instance.

4. In the upper-right corner of the page, click the Create User Group button.

   The Create User Group plane appears.

5. In the User Group Name box, type a name for the new group.

6. Add users to the group:
   a. Next to Users, click the button.

      The Add Users plane appears.

   b. For each user you want to add, click the Search by user drop-down box and begin typing a user name.

      As you type, Tenable.io filters the list of users in the drop-down box to match your search.

   c. Select a user from the drop-down box.

      Tenable.io adds the user to the list of users to be added to the user group.
d. To add the listed users, click **Add**.

7. Click **Create**.

Tenable.io creates the user group and adds the listed users as members. The **User Groups** page appears, where you can view the new group listed in the user groups table.
Edit a User Group

Required User Role: Administrator

To edit a group:

1. In the upper-left corner, click the ☐ button.
   
   The left navigation plane appears.

2. In the left navigation plane, click Settings.
   
   The Settings page appears.

3. Click the Groups tile.
   
   The User Groups page appears. This page contains a table that lists all user groups for your Tenable.io instance.

4. In the user groups table, click the user group that you want to edit.
   
   The user group detail plane appears.

5. Do any of the following:

   - Change the group name:
     a. Click the group name.
     b. Type a new group name.
     c. Click the ✓ button.

     Tenable.io saves your changes.

   - Add users to the group:
     a. Next to Users, click the + button.

     The Add Users plane appears.
b. For each user you want to add, click the **Search by user** drop-down box and begin typing a user name.

As you type, Tenable.io filters the list of users in the drop-down box to match your search.

c. Select a user from the drop-down box.

Tenable.io adds the user to the list of users to be added to the user group.

**Tip:** To remove a user from the list of users to be added, roll over the user and click the cross button.

d. Click **Add**.

Tenable.io adds the listed users to the user group.

- **Remove a user from the group:**
  
a. Under **Users**, roll over the user account you want to remove.

    The action buttons appear in the row.
  
b. Click the cross button.

    Tenable.io removes the user from the **Users** list.

6. Click **Save**.

Tenable.io saves the user group with any changes you made. The **User Groups** page appears, where you can view the updated group listed in the user groups table.
Delete a Group

**Required User Role:** Administrator

Before you begin:

- **Remove** all users from the user group. You cannot delete a user group that contains any users.

To delete one or more user groups in the new interface:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Groups** tile.
   
   The **User Groups** page appears. This page contains a table that lists all user groups for your Tenable.io instance.

4. Select the user group or groups you want to delete.
   
   - **Select a single user group.**
     
     a. In the user groups table, roll over the user group you want to delete.
     
        The action buttons appear in the row.
     
        b. Click the button.
     
        A confirmation window appears.

   - **Select multiple user groups.**
     
     a. In the user groups table, select the check box for each user group you want to delete.
The action buttons appear in the row.

b. In the action bar, click the button.

A confirmation window appears.

5. In the confirmation window, click **Delete**.

Tenable.io deletes the selected user group or groups. The deleted group or groups no longer appear in the user groups table.
Groups (Classic Interface)

**Note:** This section describes the classic Tenable.io interface. For an introduction to the new interface, see User Groups in the new interface.

To access the Groups page, click **Settings** in the top navigation bar, then click **Groups** in the left navigation bar.

The Groups page displays a table of all Tenable.io groups. This documentation refers to that table as the *groups table*.

You can assign groups permissions for scans, policies, agents, access groups, and target groups. When you assign users to a group, the users inherit the permissions assigned to the group. Your organization may utilize groups to provide permissions to batches of users based on the roles of those users and your organization's security posture.

Via the Groups page, you can:

- [Create a Group (Classic Interface)]
- [Edit a Group (Classic Interface)]
- [Delete a Group (Classic Interface)]
Create a Group (Classic Interface)

**Required User Role:** Administrator

To create a group:

1. In the top navigation bar, click **Settings**.
   The **About** page appears.

2. In the left navigation bar, click **Groups**.
   The **Groups** page appears.

3. In the upper-right corner of the page, click the **New Group** button.
   The **New Group** window appears.

4. In the **Name** box, type a name for the new group.

5. Click **Add**.
   The group is created and the **Edit Group** page appears. You can now add users to the group.
Edit a Group (Classic Interface)

**Required User Role:** Administrator

To edit a group in the classic interface:

1. In the top navigation bar, click **Settings**.
   
   The **About** page appears.
2. In the left navigation bar, click **Groups**.
   
   The **Groups** page appears.
3. In the groups table, click the name of the group that you want to edit.
   
   The **Edit Group** page appears, displaying the **Group Settings** section.
4. Do one of the following:

   - **Change the group name:**
     a. In the **Group Settings** tab, in the **Name** box, type a name for the group.
     b. Click **Save**.

   - **Add a user to the group:**
     a. Click the **Manage Users** tab.
        
        If the group already includes users, those users appear in a table.
     b. In the upper-right corner of the page, click the **Add User** button.
        
        The **Add User** window appears.
     c. In the **User** box, select the user that you want to add to the group.
        
        **Tip:** The **User** box includes a search field. In the search field, type the name of a user in order to filter the list of users.
     d. Click **Save**.
The user is added to the group and appears on the table on the Manage Users section.

- Remove a user from the group:
  a. Click the Manage Users tab.

  The groups table appears.

  b. Click the × button next to the user that you want to remove from the group.

  The Remove User window appears.

  c. Click Remove.

  Tenable.io removes the user from the group. If there are no users left in the group, the table disappears.
Delete a Group (Classic Interface)

**Required User Role:** Administrator

To delete a group:

1. In the top navigation bar, click **Settings**.
   
   The **About** page appears.

2. In the left navigation bar, click **Groups**.
   
   The **Groups** page appears.

3. In the groups table, click the ✗ button next to the group you want to delete.
   
   The **Delete Group** window appears.

4. Click **Delete**.
   
   Tenable.io deletes the group and removes it from the groups table.
Sensors Overview

**Note:** This section describes the new interface. For information about the classic interface, see [Scanners (Classic Interface)](#). For information about navigating the new interface, see [Navigate Tenable.io (New Interface)](#).

Tenable.io supports the following sensor types:

- Tenable-provided *regional cloud sensors*. For more information, see [Cloud Sensors](#).
- Manually configured *linked sensors* (Nessus scanners, NNM instances, Web Application Scanning sensors, and Nessus Agents). For more information, see [Linked Sensors](#).
Cloud Sensors

By default, Tenable provides regional cloud sensors. You can select these sensors when you create and launch scans.

The Tenable.io interface displays regional cloud sensors in the following groups:

- **US Cloud Scanner**: A group of scanners from one US-EAST range (Ohio or Virginia) and the US-WEST range.
- **US East Cloud Scanners**: A group of scanners from either the Ohio or Virginia US-EAST range.
- **US West Cloud Scanners**: A group of scanners from the US-WEST range.
- **AP Singapore Cloud Scanners**: A group of scanners from the Singapore AP-SOUTHEAST range.
- **AP Sydney Cloud Scanners**: A group of scanners from the Sydney AP-SOUTHEAST range.
- **AP Tokyo Cloud Scanners**: A group of scanners from the AP-NORTHEAST-1 range.
- **CA Central Cloud Scanners**: A group of scanners from the CA-CENTRAL-1 range.
- **EU Frankfurt Cloud Scanners**: A group of scanners from the EU-CENTRAL range.
- **UK Cloud Scanners**: A group of scanners from the EU-WEST-2 (London) range.
- **Amazon GOV-CLOUD**: A group of scanners available for Federal Risk and Authorization Management Program (FedRAMP) environments.
- **APAC Cloud Scanners**: A group of scanners from the following three AWS ranges:
  - AP-SOUTHEAST-1 (Singapore)
  - AP-SOUTHEAST-2 (Sydney)
  - AP-NORTHEAST-1 (Tokyo)
  - Amazon AP-SOUTH (Mumbai)
**EMEA Cloud Scanners**: A group of scanners from the following AWS ranges:

- Amazon EU-CENTRAL (Frankfurt)
- Amazon EU-WEST (London)

The following table identifies each Tenable.io regional cloud sensor and, for whitelisting purposes, its IP address ranges. These IP address ranges are exclusive to Tenable.

**Note**: If you use cloud connectors, Tenable recommends allowing the IP addresses for the region in which the Tenable.io site resides.

<table>
<thead>
<tr>
<th>Sensor</th>
<th>IP Range</th>
<th>IPv6 Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon CA-CENTRAL-1 (Canada)</td>
<td>35.182.14.64/26</td>
<td>2600:1f11:622:3000::/56</td>
</tr>
<tr>
<td></td>
<td>3.98.92.0/25</td>
<td></td>
</tr>
<tr>
<td>Amazon US-EAST (Ohio or Virginia)</td>
<td>13.59.252.0/25</td>
<td>2600:1f16:8ca:e900::/56</td>
</tr>
<tr>
<td></td>
<td>54.175.125.192/26</td>
<td>2600:1f18:614c:8000::/56</td>
</tr>
<tr>
<td></td>
<td>34.201.223.128/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.132.217.0/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>18.116.198.0/24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>44.192.244.0/24</td>
<td></td>
</tr>
<tr>
<td>Amazon US-WEST (California or Oregon)</td>
<td>54.219.188.128/26</td>
<td>2600:1f1c:13e:9e00::/56</td>
</tr>
<tr>
<td></td>
<td>13.56.21.128/25</td>
<td>2600:1f14:141:7b00::/56</td>
</tr>
<tr>
<td></td>
<td>34.223.64.0/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>44.242.181.128/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.101.175.0/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>35.82.51.128/25</td>
<td></td>
</tr>
<tr>
<td>Amazon EU-CENTRAL (Frankfurt)</td>
<td>54.93.254.128/26</td>
<td>2a05:d014:532:b00::/56</td>
</tr>
<tr>
<td></td>
<td>18.194.95.64/26</td>
<td></td>
</tr>
<tr>
<td>Sensor</td>
<td>IP Range</td>
<td>IPv6 Range</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td></td>
<td>3.124.123.128/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.67.7.128/25</td>
<td></td>
</tr>
<tr>
<td>Amazon EU-WEST (London)</td>
<td>35.177.219.0/26</td>
<td>2a05:d01c:da5:e800::/56</td>
</tr>
<tr>
<td></td>
<td>3.9.159.128/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>18.168.180.128/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>18.168.224.128/25</td>
<td></td>
</tr>
<tr>
<td>Amazon AP-SOUTHEAST (Singapore)</td>
<td>54.255.254.0/26</td>
<td>2406:da18:844:7100::/56</td>
</tr>
<tr>
<td></td>
<td>18.139.204.0/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>13.213.79.0/24</td>
<td></td>
</tr>
<tr>
<td>Amazon AP-SOUTHEAST (Sydney)</td>
<td>13.210.1.64/26</td>
<td>2406:da1c:20f:2f00::/56</td>
</tr>
<tr>
<td></td>
<td>3.106.118.128/25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.26.100.0/24</td>
<td></td>
</tr>
<tr>
<td>Amazon AP-NORTHEAST-1 (Tokyo)</td>
<td>13.115.104.128/25</td>
<td>2406:da14:e76:5b00::/56</td>
</tr>
<tr>
<td></td>
<td>35.73.219.128/25</td>
<td></td>
</tr>
<tr>
<td>Amazon AP-SOUTH (Mumbai)</td>
<td>3.108.37.0/24</td>
<td>2600:1f1e:9a:ba00::/56</td>
</tr>
<tr>
<td>Amazon SA-EAST (São Paulo)</td>
<td>15.228.125.0/24</td>
<td>2406:da1a:5b2:8500::/56</td>
</tr>
<tr>
<td>Amazon GOV-CLOUD</td>
<td>3.32.43.0 - 3.32.43.32</td>
<td>2600:1f12:6d3:300::/56</td>
</tr>
</tbody>
</table>

Scan ranges may also be grouped into the following categories:

<table>
<thead>
<tr>
<th>Sensor</th>
<th>IP Range</th>
<th>IPv6 Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>APAC Cloud Scanners</td>
<td>54.255.254.0/26</td>
<td>2406:da18:844:7100::/56</td>
</tr>
<tr>
<td></td>
<td>18.139.204.0/25</td>
<td>2406:da1c:20f:2f00::/56</td>
</tr>
<tr>
<td></td>
<td>13.213.79.0/24</td>
<td>2406:da14:e76:5b00::/56</td>
</tr>
</tbody>
</table>

Scan ranges may also be grouped into the following categories:
<table>
<thead>
<tr>
<th>Sensor</th>
<th>IP Range</th>
<th>IPv6 Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>◦ AP-SOUTHEAST-2 (Sydney)</td>
<td>13.210.1.64/26</td>
<td></td>
</tr>
<tr>
<td>◦ AP-NORTHEAST-1 (Tokyo)</td>
<td>3.106.118.128/25</td>
<td></td>
</tr>
<tr>
<td>◦ Amazon AP-SOUTH (Mumbai)</td>
<td>3.26.100.0/24</td>
<td>13.115.104.128/25</td>
</tr>
<tr>
<td></td>
<td>13.115.104.128/25</td>
<td>35.73.219.128/25</td>
</tr>
<tr>
<td></td>
<td>3.108.37.0/24</td>
<td></td>
</tr>
</tbody>
</table>

| EMEA Cloud Scanners                         | 54.93.254.128/26| 2a05:d014:532:b00::/56 |
| ◦ Amazon EU-CENTRAL (Frankfurt)             | 18.194.95.64/26 | 2a05:d01c:da5:e800::/56 |
| ◦ Amazon EU-WEST (London)                   | 3.124.123.128/25|                  |
|                                             | 3.67.7.128/25   |                  |
|                                             | 35.177.219.0/26 |                  |
|                                             | 3.9.159.128/25  |                  |
|                                             | 18.168.180.128/25|             |
|                                             | 18.168.224.128/25|             |

**Tip:** In addition to the above listed IP address ranges, add the following for internal scanner or agent communications:

- 162.159.129.83/32
- 162.159.130.83/32
- 2606:4700:7::a29f:8153
- 2606:4700:7::a29f:8253
- *.cloud.tenable.com with the wildcard character (*) to allow cloud.tenable.com and all subdomains, such as sensor.cloud.tenable.com

If you do not include these ranges, the sensor automatically fails over to the aforementioned regional cloud sensors.
Linked Scanners

After you install a Nessus scanner, NNM instance, Tenable.io Web Application Scanning sensor, or Nessus Agent sensor, you can link it to Tenable.io.

Before you can use linked scanners in Tenable.io scans, you must:
1. Install the appropriate Tenable product on the sensor or the host you want to scan.

<table>
<thead>
<tr>
<th>Sensor Type</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nessus Agent</td>
<td>• Environments</td>
</tr>
<tr>
<td></td>
<td>• Install Nessus Agent in the Nessus Agent Deployment and User Guide</td>
</tr>
<tr>
<td>Industrial Security</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Industrial Security is end-of-life (EOL). For information about EOL dates and</td>
</tr>
<tr>
<td></td>
<td>policies for Tenable products, see the Tenable Software Release Lifecycle Matrix</td>
</tr>
<tr>
<td></td>
<td>and Policy.</td>
</tr>
<tr>
<td>Nessus Network Monitor</td>
<td>• Environments</td>
</tr>
<tr>
<td></td>
<td>• Install Nessus Network Monitor in the Nessus Network Monitor User Guide</td>
</tr>
<tr>
<td></td>
<td>• Deploy or Install Tenable Core + Nessus Network Monitor in the Tenable Core User</td>
</tr>
<tr>
<td></td>
<td>Guide</td>
</tr>
<tr>
<td>Nessus</td>
<td>• Environments</td>
</tr>
<tr>
<td></td>
<td>• Install Nessus in the Nessus User Guide</td>
</tr>
<tr>
<td></td>
<td>• Deploy or Install Tenable Core + Nessus in the Tenable Core User Guide</td>
</tr>
<tr>
<td></td>
<td>Note: If a Nessus scanner has multiple NICs/interfaces, you may see multiple IPv4/IPv6 addresses for the scanner.</td>
</tr>
<tr>
<td>Tenable.io Web Application</td>
<td>• Environments</td>
</tr>
<tr>
<td>Scanner</td>
<td>• Deploy or Install Tenable Core + Web Application Scanning in the Tenable Core</td>
</tr>
<tr>
<td></td>
<td>User Guide</td>
</tr>
</tbody>
</table>

2. Link the sensor or link the agent to Tenable.io.

After linking a scanner, you can:
- **View** a list of your linked scanners.
- **View** sensor details.
- **Modify** sensor settings.
- **Modify** sensor permissions.
- **Enable or disable** a sensor.
- **Remove** a sensor.
- **Manage** sensors in scanner groups.
- **Manage** agents.
- **Manage** networks.
View Linked Scanners

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

To view your linked scanners:

1. In the upper-left corner, click the \(\equiv\) button.
   
The left navigation plane appears.
2. In the left navigation plane, click **Settings**.
   
The **Settings** page appears.
3. Click the **Sensors** tile.
   
The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.
4. Click the **Linked Scanners** tab.
   
   A list of your linked scanners appears. By default, **Nessus Scanners** is selected in the left navigation menu.
5. To view a different type of linked scanners, in the left navigation menu, click the type of linked scanners you want to view.
   
   Tenable.io displays the selected type of linked scanners.
Download Linked Scanner Logs

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

In Tenable.io, you can request and download a log file containing logs and system configuration data from any of your linked scanners. This information can help you troubleshoot system problems and easily provide data for Tenable Support.

You can store a maximum of five log files from each scanner. Once the limit is reached, you must remove an old log file to download a new one.

To download logs from a linked scanner in Tenable.io:

1. In the upper-left corner, click the **button.
   
The left navigation plane appears.
2. In the left navigation plane, click **Settings**.
   
The **Settings** page appears.
3. Click the **Sensors** tile.
   
The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.
4. Click the **Linked Scanners** tab.
   
The linked scanners table appears.
5. In the linked scanners table, click the scanner for which you want to download logs.
   
The details page for that scanner appears.
6. Click the **Logs** tab.
   
A table displays any previously downloaded logs.
7. In the upper-right corner, click **Request Logs**.

**Note:** If you have reached the maximum of five log files, the **Request Logs** button is disabled. Remove an existing log before downloading a new one.
The pending log appears as a row in the logs table. Tenable.io requests the logs from the scanner the next time it checks in, which may take several minutes.

8. In the row for an available log file, click the \( \downarrow \) button.

Your system downloads the log file.

To remove an existing log:

1. In the row of the log you want to remove, click the \( \text{🗑} \) button.

A confirmation window appears.

2. In the confirmation window, click **Delete**.

Tenable.io deletes the log and removes it from the table.

To cancel a pending or failed log request:

1. In the row of the pending or failed log request that you want to cancel, click the \( \text{🚫} \) button.

Tenable.io cancels the log request and removes it from the table.
Link a Sensor

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Manager or Administrator

This procedure describes how to link a sensor to Tenable.io.

Linking a sensor to Tenable.io represents a one-time event in managing a sensor, unless you remove the sensor. After you link the sensor, the sensor connects to Tenable.io using unique credentials.

Once you copy the linking key in Tenable.io, you must paste the linking key in the appropriate location of the sensor user interface (e.g. the Nessus Agent CLI or the NNM Cloud Settings section). Expand the following sections for specific details.

**Note:** Under certain circumstances, you may need to regenerate the linking key. See [Regenerate a Linking Key](#) for more information.

To link a sensor in the new interface:

1. In the upper-left corner, click the ☐️ button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Sensors** tile.
   
   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. Then:
   
   To link a Nessus Agent sensor, in the left navigation menu, click **Agents**.
   
   a. In the upper-right corner of the page, click ☑️ **Add Agent**.

   The **Add Agent** plane appears.
b. Do one of the following:

- To manually install and link Nessus Agent:
  a. In the **Linking Key** section, click **Copy**.

    A **Linking key copied to clipboard** confirmation message appears.

  b. Access the Nessus Agent instance that you want to link to Tenable.io.

  c. Use the copied linking key in the Nessus Agent CLI to link the sensor. For more information, see [Install Nessus Agent](#) in the *Nessus Agent Deployment and User Guide*.

- (Linux only) To use a single command to install and link Nessus Agent:
  a. Under the **One-Line Installation** instructions, copy the command.

    The command contains the linking key and syntax required to install the agent, link the agent to Tenable.io, change the agent name, and add the agent to an agent group. For example:

    ```bash
    curl -H 'X-Key: abcd1234efgh5678ijkl9012mnop3456qrst7890uvwxyz1234yz5678abcd1234ef' 'https://cloud.tenable.com/install/agent?name=agent-name&groups=agent-group' | bash
    ```

    b. In the command, replace *agent-name* with the agent name.

    **Tip:** If you do not want to set a custom agent name, remove `name=agent-name`. If you do not set a custom name, Tenable names the agent using the hostname of the machine on which the agent is installed.

  c. In the command, replace *agent-group* with the agent group name.

    **Note:** The agent group name is case-sensitive and must match exactly.
Tip: If you do not want to add the agent to an agent group, remove groups=agent-group.

d. As a user with administrative privileges, access the CLI of the Linux machine on which you want to install the agent.

e. Run the command.

Nessus Agent installs on your Linux machine, links to your instance of Tenable.io, and updates the agent name and agent group if necessary.

To link an Industrial Security instance, in the left navigation menu, click Industrial Security.

Industrial Security is end-of-life (EOL). For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

a. In the upper-right corner of the page, click Add Industrial Security.

The Add Industrial Security plane appears.

b. In the Linking Key section, click Copy.

A Linking key copied to clipboard confirmation message appears.

c. Access the Industrial Security instance that you want to link to Tenable.io.

d. Use the copied linking key in the Industrial Security user interface to link the sensor.

To link an NNM instance, in the left navigation menu, click NNM.

a. In the upper-right corner of the page, click Add NNM.

The Add Nessus Network Monitor plane appears.

b. In the Linking Key section, click Copy.

A Linking key copied to clipboard confirmation message appears.

c. Access the NNM instance that you want to link to Tenable.io.

d. Use the copied linking key in the NNM user interface to link the sensor. For more information, see the NNM User Guide.
To link a Nessus sensor, in the left navigation menu, click **Nessus Scanners**.

a. In the upper-right corner of the page, click **Add Scanner**.

The **Add Nessus** plane appears.

b. Do one of the following:

- To manually install and link Nessus:
  a. In the **Linking Key** section, click **Copy**.

    A **Linking key copied to clipboard** confirmation message appears.
  b. Access the Nessus instance that you want to link to Tenable.io.
  c. Use the copied linking key in the Nessus user interface to link the sensor. For more information, see the [Link to Tenable.io](#) in the **Nessus User Guide**.

- (Linux only) To use a single command to install and link a Nessus scanner:
  a. Under the **One-Line Installation** instructions, copy the command.

    The command contains the linking key and syntax required to install the scanner, link the scanner to Tenable.io, change the scanner name, and add the scanner to a scanner group. For example:

    ```
    curl -H 'X-Key: abcd1234efgh5678ijkl9012mnop3456qrst7890uvwx1234yz5678abcd1234ef' 'https://cloud.tenable.com/install/scanner?name=scanner-name&groups=scanner-group'| bash
    ```
  b. In the command, replace `scanner-name` with the scanner name.

    **Tip:** If you do not want to set a custom scanner name, remove `name-e=scanner-name`. If you do not set a custom name, Tenable names the scanner using the hostname of the machine on which the scanner is installed.
  c. In the command, replace `scanner-group` with the scanner group name.
Note: The scanner group name is case-sensitive and must match exactly.

Tip: If you do not want to add the scanner to an scanner group, remove groups=scanner-group.

d. As a user with administrative privileges, access the CLI of the Linux machine on which you want to install the scanner.

e. Run the command.

Nessus installs on your Linux machine, links to your instance of Tenable.io, and updates the scanner name and scanner group if necessary.

To link a Tenable Core + Tenable.io Web Application Scanning instance, in the left navigation menu, click WAS.

a. In the upper-right corner of the page, click Add WAS.

The Add WAS plane appears.

b. In the Linking Key section, click Copy.

A Linking key copied to clipboard confirmation message appears.

c. Access the Tenable Core + Tenable.io Web Application Scanning instance that you want to link to Tenable.io.

d. Use the copied linking key in the Tenable Core + Tenable.io Web Application Scanning user interface to link the sensor. For more information, see the Tenable Core+ Tenable.io Web Application Scanning User Guide.

What to do next:

- Manage the sensor in Tenable.io (including disabling or re-enabling the sensor link).

- Select the sensor when configuring Tenable.io scans.
Regenerate a Linking Key

Required Tenable.io Vulnerability Management User Role: Scan Manager or Administrator

Required Tenable.io Web Application Scanning User Role: Scan Manager or Administrator

Under certain circumstances, you may need to regenerate the linking key for your Tenable.io instance. For example, you may regenerate the key for security reasons if an employee with knowledge of the linking key leaves your organization.

Regenerating a linking key does not affect sensors that are currently linked to Tenable.io, because the linking key is only used to establish the initial link. After you link a sensor, the sensor connects to Tenable.io using unique credentials.

If your organization has hard-coded a linking key into implementation scripts, keep in mind the following:

- Be sure to replace the original key with the regenerated key to prevent script failure.
- Each Tenable.io instance uses a single linking key for all sensor types. If you regenerate the linking key while working with one type of sensors (for example, Nessus scanners), you also regenerate the linking key for the other sensor types. If you regenerate the linking key, be sure to update implementation for scripts involving all types of sensors.

To regenerate a linking key for your Tenable.io instance in the new interface:

1. In the upper-left corner, click the button.
   
The left navigation plane appears.

2. In the left navigation plane, click Settings.
   
The Settings page appears.

3. Click the Sensors tile.
   
The Sensors page appears. By default, Nessus Scanners is selected in the left navigation menu and the Cloud Scanners tab is active.
4. In the left navigation menu, click any sensor type (for example, **NNM**).
   
The appropriate sensor page appears.
5. In the upper-right corner of the page, click the **Add [Sensor Type]** button (for example, **Add NNM**).
   
The appropriate sensor plane appears (for example, **Add NNM**).
6. In the **Add [Sensor Type]** plane, click the **Regenerate** button.
   
A confirmation window appears.
7. In the confirmation window, click **Regenerate**.
   
The **Regenerated Linking Key** message appears, and the new linking key replaces the original linking key in the **Add [Sensor Type]** plane.

What to do next:

- **Link** a sensor.
View Sensor Details

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

You can view details for both cloud sensors and linked sensors.

To view sensor details in the new interface:

1. In the upper-left corner, click the ☰ button.
   
   The left navigation plane appears.

2. In the left navigation plane, click Settings.
   
   The **Settings** page appears.

3. Click the Sensors tile.
   
   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. In the left navigation bar, click the sensor type you want to view.
   
   A table of sensors appears.

5. For **Nessus Scanners**, do one of the following:
   
   - Click the **Cloud Scanners** tab to view cloud scanners connected to Tenable.io. For more information, see [Cloud Scanners](#).
   
   - Click the **Linked Scanners** tab to view on-premises scanners linked to Tenable.io. For more information, see [Linked Scanners](#).

6. In the sensors table, click the sensor where you want to view details.
   
   The **Details** page appears.

   Depending on the sensor type, you can do the following in the **Details** page:
   
   - Click the **Settings** tab to modify sensor settings.
   
   - Click the **Permissions** tab to modify sensor permissions.
Edit Sensor Settings

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Industrial Security is end-of-life (EOL). For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle [Matrix](#) and [Policy](#).

You can edit certain settings for the following types of linked sensors:

- Nessus Network Monitor
- Nessus for Amazon Web Service (AWS)

To edit sensor settings in the new interface:

1. In the upper-left corner, click the ☰ button.
   
The left navigation plane appears.
2. In the left navigation plane, click **Settings**.
   
The **Settings** page appears.
3. Click the **Sensors** tile.
   
The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.
4. In the left navigation bar, click the appropriate sensor type.
   
The sensor table appears.
5. If the sensor is a **Nessus Scanner**, do one of the following:
   
   - Click the **Cloud Scanners** tab to view cloud scanners connected to Tenable.io. For more information, see [Cloud Scanners](#).
   
   - Click the **Linked Scanners** tab to view scanners linked to Tenable.io. For more information, see [Linked Scanners](#).
6. In the table of linked sensors, click the sensor for which you want to edit settings.
   
The sensor details appear. By default, the **Overview** tab is active.
7. Click the **Settings** tab.
   The sensor settings appear.

8. Edit the **sensor settings**.

9. In the lower-right corner of the page, click **Save**.
## Sensor Settings

Industrial Security is end-of-life (EOL). For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

You can modify certain settings for the following types of linked sensors:

- Nessus Network Monitor
- Nessus for Amazon Web Service (AWS)

These settings are described in the table below.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Sensor Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Frequency</td>
<td>NNM</td>
<td>Specifies the frequency, in minutes, that you want the sensor to report information to Tenable.io.</td>
</tr>
<tr>
<td>Software Update Type</td>
<td>NNM (5.6.1 and later only)</td>
<td>Specifies which components, if any, you want NNM to automatically update.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>All components</strong> includes web server, HTML client, plugins, and engine.</td>
</tr>
<tr>
<td>Updates instances every (minutes)</td>
<td>AWS</td>
<td>Specifies the frequency, in minutes, that you want the AWS sensor to report information to Tenable.io about the instances it has access to.</td>
</tr>
</tbody>
</table>
Edit Sensor Permissions

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Manager or Administrator

You can set the following Tenable.io user permissions levels in your sensor configuration:

- **No Access** – The user or group cannot use the scanner in scan configurations or edit the scanner configuration.
- **Can Use** – The user or group can use the scanner in scan configurations, but cannot edit the scanner configuration.
- **Can Manage** – The user or group can use the scanner in scan configurations and edit the scanner configuration.

To modify sensor permissions in the new interface:

1. In the upper-left corner, click the **☰** button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Sensors** tile.
   
   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. In the left navigation bar, click the appropriate sensor type.
   
   A sensors table appears.

5. If the sensor is a **Nessus Scanner**, click the **Linked Scanners** tab to view on-premises scanners linked to Tenable.io. For more information, see [Linked Scanners](#).

6. In the table of linked sensors, click the sensor for which you want to set permissions.
The **Details** page appears. For all sensors except agents, the **Overview** tab is active by default.

7. Click the **Permissions** tab.

   **Note:** By default, any user in your Tenable.io instance can use the scanner.

8. Do any of the following:

   - To select a permissions level from the drop-down box for the **Default** user.

   - To specify permissions for an individual user or user group:
     a. In the **Add users or user groups** text box, type the name of a user or user group. As you type, Tenable.io searches for matches to existing users or user groups.
     b. In the search results, select a user or user group.
     c. In the permissions drop-down, select a permissions level for the user or user group you added.

9. In the lower-right corner of the page, click **Save**.
Enable or Disable a Sensor

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Manager or Administrator

To enable or disable a sensor in the new interface:

1. In the upper-left corner, click the ☐ button.
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   The **Settings** page appears.

3. Click the **Sensors** tile.
   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. In the left navigation bar, click the appropriate sensor type.
   The sensors table appears.

5. (Optional) If the sensor is a **Nessus Scanner**, click the **Linked Scanners** tab to view on-premises scanners linked to Tenable.io. For more information, see **Linked Scanners**.

6. In the table of linked sensors, roll over the sensor you want enable or disable.
   The action buttons appear in the row.

7. Do one of the following:
   - To enable a sensor, click the ☑ button.
   - To disable a sensor, click the ☐ button.

Tenable.io enables or disables the sensor.
Remove a Sensor

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Manager or Administrator

**Note:** You cannot remove cloud sensors.

To remove a sensor in the new interface:

1. In the upper-left corner, click the button.
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   The **Settings** page appears.

3. Click the **Sensors** tile.
   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. In the left navigation bar, click the appropriate sensor type.
   The sensor table appears.

5. For **Nessus Scanners**, click the **Linked Scanners** tab to view on-premises scanners linked to Tenable.io. For more information, see **Linked Scanners**.

6. In the table of linked sensors, roll over the sensor you want to remove.
   The action bar appears at the bottom of the page.

7. Click the button.
   A confirmation window appears.

8. Click **Delete** to confirm the removal.
   Tenable.io removes the sensor from the list.
Scanner Groups

**Note:** This section describes the new interface. For information about the classic interface, see [Scanners (Classic Interface)](#). For information about navigating the new interface, see [Navigate Tenable.io (New Interface)](#).

You can use scanner groups to organize and manage the scanners linked to your Tenable.io instance. For example, you can add all sensors related to a specific geographical location to a group, for example, a group named "East Coast Scanners."

You can add a scanner to one or more scanner groups.

When you create a scan, you can select the scanner group to use to launch the scan. Alternatively, you can select **Auto-Select** to enable **scan routing** for the scan, which assigns scans to scanners based on the targets configured in scanner groups.

Tenable.io determines which scanner in a scanner group to use based on the following criteria:

- The scanner is active and has communicated to Tenable.io within the last 5 minutes.
- The scanner is running the lowest number of active scans and is scanning the lowest number of hosts.

**Note:** If your organization uses scan networks, you can only add scanners to scanner groups that belong to the same network. For more information, see [Networks](#).

**Note:** If a remote scanner is part of a **Scanner Group** and is unlinked during its operations, the scan's operations complete, but Tenable.io does not include the unlinked scanner for future use.

For more information on **Scanner Groups**, see the following topics:

- [Create a Scanner Group](#)
- [Modify a Scanner Group](#)
- [Configure User Permissions for a Scanner Group](#)
- [Delete a Scanner Group](#)
- [Add a Sensor to a Scanner Group](#)
- [Remove a Sensor from a Scanner Group](#)
• View Sensors in a Scanner Group

• View All Scans for a Sensor
Create a Scanner Group

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

To create a scanner group in the new interface:

1. In the upper-left corner, click the button.  
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.  
   The **Settings** page appears.

3. Click the **Sensors** tile.  
   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. Click the **Scanner Groups** tab.  
   The **Scanner Groups** tab appears. This tab contains a table listing existing scanner groups.

5. In the upper-right corner, click the button.  
   The **Add Scanner Group** plane appears.

6. In the **Group Name** field, type a name for the group.

7. (Optional) In the **Targets for Scan Routing** box, type a comma-separated list of scan routing targets.  
   Targets in the list must be in the supported formats.  
   This list specifies the targets that scanners in this scanner group can scan if a scan is configured to use the **Auto-Select** scanner. For more information, see Example: Scan Routing.

   **Note:** You can specify up to 10,000 individual scan routing targets for an individual scanner group. For example, 192.168.0.1, example.com, *.example.net, 192.168.0.0/24 specifies four scan routing targets. To condense a scan routing target list, Tenable recommends using wildcard and range formats, instead of individual IP addresses.

8. (Optional) **Configure** user permissions for a scanner group.
By default, in any new scanner group, Tenable.io assigns the system-generated All Users group Can Use permissions.

9. Click Save.

If Targets for Scan Routing specifies more than the maximum number of targets, an error message appears. Condense the scan routing targets by using wildcard and range formats instead of individual IP addresses, then try again to save the scanner group.

In all other cases, the new group appears in the Scanner Groups list.
Modify a Scanner Group

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

To modify a scanner group in the new interface:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.
2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.
3. Click the **Sensors** tile.
   
   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.
4. Click the **Scanner Groups** tab.
   
   The **Scanner Groups** tab appears. This tab contains a table listing the scanner groups you have permission to use or manage.
5. (Optional) Search the table for the group you want to modify. For more information, see [Tenable.io Tables](#).
6. In the scanner group table, roll over the scanner group you want to modify.
7. Click the button.
   
   The scanner group plane appears.
8. Modify any of the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a new name.</td>
</tr>
<tr>
<td>User and Group Permissions</td>
<td>Configure user permissions for the scanner group.</td>
</tr>
</tbody>
</table>
9. (Optional) In the **Targets for Scan Routing** box, type a comma-separated list of scan routing targets.

    Targets in the list must be in the [supported formats](#).

    This list specifies the targets that scanners in this scanner group can scan if a scan is configured to use the **Auto-Select** scanner. For more information, see [Example: Scan Routing](#).

    **Note:** You can specify up to 10,000 individual scan routing targets for an individual scanner group. For example, 192.168.0.1, example.com, *.example.net, 192.168.0.0/24 specifies four scan routing targets. To condense a scan routing target list, Tenable recommends using wildcard and range formats, instead of individual IP addresses.

10. Click **Save**.

    If **Targets for Scan Routing** specifies more than the maximum number of targets, an error message appears. Condense the scan routing targets by using wildcard and range formats instead of individual IP addresses, then try again to save the scanner group.

    In all other cases, Tenable.io updates the scanner group with your changes.

To assign scanners to a scanner group in the new interface:

1. In the upper-left corner, click the **button.

    The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

    The **Settings** page appears.

3. Click the **Sensors** tile.

    The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. (Optional) For WAS, in the left navigation menu, click **WAS**.

    The **Linked Scanners** tab appears.

5. Click the **Scanner Groups** tab.
The **Scanner Groups** tab appears. This tab contains a table listing the scanner groups you have permission to use or manage.

6. In the scanner groups table, click the row of the scanner group where you want to add scanners.

The **Group Details** page appears.

7. Click **Assign Scanners**.

The **Assign Scanner** page appears.

8. (Optional) Search the table for the scanner you want to assign. For more information, see [Interact with a Standard Table](#).

9. In the scanners table, select the check boxes next to the scanner or scanners you want to add to the scanner group.

10. Click **Assign**.

If the assignment is successful, Tenable.io adds the scanner to the scanner group, and the **Group Details** page appears.

If Tenable.io encounters any problems during processing, the **Assign Scanners** page remains active, and one of the following messages appears in the **Assignment** column of the affected scanner:

<table>
<thead>
<tr>
<th>Possible Error Messages</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>This sensor already exists in the scanner group.</td>
<td>Click <strong>Cancel</strong> to close the page.</td>
</tr>
<tr>
<td>An error occurred adding this sensor to the scanner group.</td>
<td>Click <strong>Assign</strong> again. If the processing still fails, contact Tenable Support.</td>
</tr>
</tbody>
</table>
Configure User Permissions for a Scanner Group

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

You can configure scanner group permissions for individual users or a user group. If you configure scanner group permissions for a user group, you assign all users in that group the same permissions. For more information, see User Groups.

You can assign the following scanner group permissions to a user or user group:

- **No Access** – *(All Users user group only)* No users (except for users or groups you specifically assign permissions) can use the scanner group in scan configurations.

- **Can Use** – The user or user group can use the scanner group in scan configurations. The user or user group can view but not edit the scanner group configuration.

- **Can Manage** – The user or user group can use the scanner group in scan configurations. The user or user group can view and edit the scanner group configuration.

To configure user permissions for a scanner group:

1. [Create](#) or [edit](#) a scanner group.

2. During scanner group configuration, in the **Users & Groups** section, do any of the following:

   - **Edit permissions for the All Users user group.**
     a. Next to the permission drop-down for the *All Users* group, click the **button.
     b. Select a permissions level.

   - **Add a user or user group to the scanner group.**
     a. In the **User & Groups** heading, click the **button.

     The **Add Users & Group** plane appears.

     b. In the **Search** field, type or click the drop-down to find and add a user or group.

**Tip:** Tenable recommends assigning permissions to user groups, rather than individual users, to minimize maintenance as individual users leave or join your organization.
Added users and groups appear below the Search field.

c. Click the Add button.

The scanner group plane appears.

By default, Tenable.io assigns the added user or user group Can Use permissions.

• **Edit permissions for an existing user or user group.**
  
  a. Next to the permissions drop-down for the user or user group you want to edit, click the ▼ button.

  b. Select a permissions level.

• **Remove a user or user group from the scanner group.**
  
  a. Roll over the user or group you want to remove.

  b. Click the ✗ button next to the user or user group.

The user or group disappears from the Users & Groups list.

3. Click Save.

Tenable.io saves your changes to the scanner group.

What to do next:

• **Use** the scanner group in a scan configuration.
Delete a Scanner Group

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

To delete one or more scanner groups:

1. In the upper-left corner, click the button.
   
The left navigation plane appears.
2. In the left navigation plane, click **Settings**.
   
The **Settings** page appears.
3. Click the **Sensors** tile.
   
The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.
4. Click the **Scanner Groups** tab.
   
The **Scanner Groups** tab appears. This tab contains a table listing existing scanner groups.
5. In the scanner groups table, select one or more scanner groups to delete:
   
   • **Select a single scanner group:**
     
     a. In the scanner groups table, roll over the scanner group you want to delete.
     
     b. Click the button next to the scanner group you want to delete.

     A confirmation window appears.
   
   • **Select multiple scanner groups:**
     
     a. In the scanner groups table, select the check boxes next to the scanner groups you want to delete.

     The action bar appears at the bottom of the page.
b. In the action bar, click the button.

A confirmation window appears.

6. In the confirmation window, click the **Delete** button.

Tenable.io deletes the group or groups you selected.
Add a Sensor to a Scanner Group

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

You can add the following types of sensors to a scanner group:

<table>
<thead>
<tr>
<th>Sensor Type</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-premises Nessus</td>
<td>yes</td>
</tr>
<tr>
<td>On-premises Tenable.io Web Application Scanning</td>
<td>yes</td>
</tr>
<tr>
<td>Tenable.io cloud</td>
<td>no</td>
</tr>
<tr>
<td>Nessus sensor for Amazon Web Services (AWS)</td>
<td>no</td>
</tr>
<tr>
<td>Nessus Network Monitor (NNM)</td>
<td>no</td>
</tr>
<tr>
<td>Nessus Agent</td>
<td>no (see <a href="#">Agent Groups</a>)</td>
</tr>
</tbody>
</table>

To add sensor to one or more scanner groups in the new interface:

1. In the upper-left corner, click the **button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Sensors** tile.

   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. Click the **Linked Scanners** tab.

   The **Linked Scanners** tab appears.

5. (Optional) Search for the scanner you want to add to a scanner group.

6. Select the scanners you want to add and the groups you want to add the scanners to:
• Add a single scanner to a group or groups.
  a. In the scanner table, roll over the sensor you want to add to a scanner group.
     The action buttons appear in the row.
  b. In the row, click the button.
     The Add to Groups plane appears.
  c. In the search box, type the name of the scanner group where you want to add the
     scanner.
  d. In the drop-down box of matching groups, click a group.
  e. (Optional) Repeat steps c and d to add additional scanner groups.

• Add multiple scanners to a group or groups.
  a. In the scanner table, select the check boxes next to the scanners you want to add
     to scanner groups.
     The action bar appears at the bottom of the page.
  b. Click the button.
     The Add to Groups plane appears.
  c. In the search box, type the name of the scanner group where you want to add the
     scanner.
  d. In the drop-down list of matching groups, click a group.
  e. (Optional) Repeat steps c and d to add additional scanner groups.

7. Click Save to save your changes.

   Tenable.io adds the scanner or scanners to the selected group or groups and closes the Add
   to Groups plane.
Remove a Sensor from a Scanner Group

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Manager or Administrator

To remove a sensor from a scanner group in the new interface:

1. In the upper-left corner, click the ☰ button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Sensors** tile.
   
   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. Click the **Scanner Groups** tab.
   
   The **Scanner Groups** tab appears. This tab contains a table listing the scanner groups you have permission to use or manage.

5. (Optional) Search the table for the group you want to modify. For more information, see [Tenable.io Tables](#).

6. In the scanner group table, click the scanner group you want to modify.
   
   The **Group Details** page appears. This page contains a table listing sensors assigned to this group.

7. (Optional) Search for the sensor you want to remove. For more information, see [Tenable.io Tables](#).

8. Select the sensor or sensors you want to remove:

9. Select the sensors you want to remove:
• Select a single sensor:
  a. In the sensors table, roll over the sensor you want to remove.
     The action buttons appear in the row.
  b. In the row, click the delete button.
     A confirmation window appears.

• Select multiple sensors:
  a. In the sensors table, select the check box for each sensor you want to remove from the group.
     The action bar appears at the bottom of the page.
  b. In the action bar, click the delete button.
     A confirmation window appears.

10. In the confirmation window, click Remove.

Tenable.io removes the sensor or sensors from the scanner group.
View Sensors in a Scanner Group

Required Tenable.io Vulnerability Management User Role: Scan Manager or Administrator

To view sensors assigned to a scanner group in the new interface:

1. In the upper-left corner, click the ☐️ button.

   The left navigation plane appears.

2. In the left navigation plane, click Settings.

   The Settings page appears.

3. Click the Sensors tile.

   The Sensors page appears. By default, Nessus Scanners is selected in the left navigation menu and the Cloud Scanners tab is active.

4. Click the Scanner Groups tab.

   The Scanner Groups tab appears. This tab contains a table listing existing scanner groups.

5. (Optional) Search the table for the group you want to view. For more information, see Tenable.io Tables.

6. In the scanner group table, click the scanner group you want to view.

   The Group Details page appears. This page contains a table listing sensors assigned to this group.
View All Scans for a Sensor

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

**Note:** You can only view all scans for sensors in **Nessus Scanners** scanner groups.

To view all scans for a sensor in the new interface:

1. [View](#) the sensors in the appropriate scanner group.

2. In the sensors table, click the sensor for which you want to view all scans.
   - The scanner **Details** page appears.

3. Click the **Manage Scans** tab.
   - Tenable.io displays a list of all scans for the sensor.
Agents

Note: This section describes the new interface. For information about the classic interface, see Agents (Classic Interface). For information about navigating the new interface, see Navigate Tenable.io (New Interface).

Agents increase scan flexibility by making it easy to scan assets without needing ongoing host credentials or assets that are offline. Additionally, agents enable large-scale concurrent scanning with little network impact.

After you install a **Nessus Agent** on a host and link the Agent to Tenable.io, the Agent appears on the Tenable.io **Linked Agents** page.

For more information, see the following topics:

- [Retrieve the Nessus Agent Linking Key](#)
- [Restart an Agent](#)
- [Unlink an Agent](#)
- [Add an Agent to an Agent Group](#)
- [Manage an Agent’s Settings](#)
- [Agent Status](#)
- [Export Agents](#)
- [Agent Filters](#)
- [Agent Groups](#)
- [Blackout Windows](#)
Retrieve the Nessus Agent Linking Key

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Before you begin the Nessus Agents installation process, you must retrieve the Nessus Agent Linking Key from Tenable.io.

To retrieve the linking key in the new interface:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Sensors** tile.
   
   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. In the left navigation menu, click **Agents**.
   
   The **Agents** page appears and the **Linked Agents** tab is active.

5. In the upper-right corner of the page, click **Add Agent**.
   
   The **Add Agent** plane appears.

6. Click the **Copy** button to copy the **Linking Key**.
   
   A **Linking key copied to clipboard** confirmation message appears.

What to do next:

- Install **Nessus Agent**.
Download Linked Agent Logs

Required Tenable.io Vulnerability Management User Role: Scan Manager or Administrator

In Tenable.io, you can request and download a log file containing logs and system configuration data from any of your linked agents. This information can help you troubleshoot system problems and easily provide data for Tenable Support.

You can store a maximum of five log files from each agent. Once the limit is reached, you must remove an old log file to download a new one.

To download logs from a linked agent in Tenable.io:

1. In the upper-left corner, click the button.
   The left navigation plane appears.
2. In the left navigation plane, click Settings.
   The Settings page appears.
3. Click the Sensors tile.
   The Sensors page appears. By default, Nessus Scanners is selected in the left navigation menu and the Cloud Scanners tab is active.
4. In the left navigation menu, click Agents.
   The Agents page appears and the Linked Agents tab is active.
5. In the agents table, click the agent for which you want to download logs.
   The details page for that agent appears.
6. Click the Logs tab.
   A table displays any previously downloaded logs.
7. In the upper-right corner, click Request Logs.

Note: If you have reached the maximum of five log files, the Request Logs button is disabled. Remove an existing log before downloading a new one.
Tenable.io requests the logs from the agent the next time it checks in, which may take several minutes. You can view the status of the request in the user interface until the download is complete.

8. To download the log file, click the ↘ button.

   The system downloads the log file.

To remove an existing log:

1. In the row of the log you want to remove, click the 🗑 button.

   A confirmation window appears.

2. In the confirmation window, click Delete.

   Tenable.io deletes the log and removes it from the table.

To cancel a pending or failed log request:

• In the row of the pending or failed log request that you want to cancel, click the 🚹 button.

   Tenable.io cancels the log request and removes it from the table.
**Restart an Agent**

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

In Tenable.io, you can restart linked agents (versions 7.6 and later) on the **Linked Agents** tab.

1. In the upper-left corner, click the **button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Sensors** tile.

   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. In the left navigation menu, click **Agents**.

   The **Agents** page appears and the **Linked Agents** tab is active.

5. (Optional) Search for a specific agent or **filter** the agents in the table.

6. Do one of the following:

   **To restart a single agent:**
   
   a. In the agents table, in the row for the agent you want to restart, click the **button.

      The **Restart Agent** window appears.

   b. Select one of the following **Restart Types**:

      | Restart Type | Description                                      |
      |--------------|--------------------------------------------------|
      | **Soft**     | Restart the agent backend without restarting the service. |
      | **Hard**     | Restart the agent backend and service.            |
      | **Idle**     | Restart the agent backend and service when the agent is not running a scan. |
c. Click **Save**.

   Tenable.io saves your settings, and the changes take effect the next time the agent checks in. For online agents, this can take up to 45 minutes.

**To restart multiple agents:**

a. Do one of the following:

   - In the agents table, select the check box next to each agent you want to restart.
   - In the table header, select the check box to select the entire page.

   The action bar appears at the bottom of the page.

   **Tip:** In the action bar, select **Select All Pages** to select all linked agents.

b. In the action bar, click the **↻** button.

   The **Restart Agents** window appears.

c. Select one of the following **Restart Types**:

<table>
<thead>
<tr>
<th>Restart Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Soft</td>
<td>Restart the agent backend without restarting the service.</td>
</tr>
<tr>
<td>Hard</td>
<td>Restart the agent backend and service.</td>
</tr>
<tr>
<td>Idle</td>
<td>Restart the agent backend and service when the agent is not running a scan.</td>
</tr>
</tbody>
</table>

d. Click **Save**.

   Tenable.io saves your settings, and the changes take effect the next time the agent checks in. For online agents, this can take up to 45 minutes.
Unlink an Agent

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

When you manually unlink an agent, the agent is removed from the **Agents** page, but the system retains related data for the period of time specified in **agent settings**. When you manually unlink an agent, the agent does not automatically relink to Tenable.io.

**Tip:** You can configure agents to automatically unlink if they are inactive for a certain number of days, as described in **agent settings**.

To manually unlink a single agent in Tenable.io in the new interface:

1. In the upper-left corner, click the **button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Sensors** tile.

   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. In the left navigation menu, click **Agents**.

   The **Agents** page appears and the **Linked Agents** tab is active.

5. (Optional) Search for a specific agent or **filter** the agents in the table. For filter descriptions, see **Agent Filters**.

6. In the agents table, in the row for the agent that you want to unlink, click the ** button.

   A confirmation window appears.

7. Click the **Unlink** button.

   Tenable.io unlinks the agent.

To manually unlink multiple agents in Tenable.io in the new interface:
1. In the upper-left corner, click the ≡ button.

   The left navigation plane appears.

2. In the left navigation plane, click Settings.

   The Settings page appears.

3. Click the Sensors tile.

   The Sensors page appears. By default, Nessus Scanners is selected in the left navigation menu and the Cloud Scanners tab is active.

4. In the left navigation menu, click Agents.

   The Agents page appears and the Linked Agents tab is active.

5. (Optional) Search for a specific agent or filter the agents in the table. For filter descriptions, see Agent Filters.

6. Do one of the following:

   • In the agents table, select the check box next to each agent you want to restart.
   • In the table header, select the check box to select the entire page.

   An action bar appears at the bottom of the page.

   Tip: In the action bar, select Select All Pages to select all linked agents.

7. In the action bar, click the button.

   A confirmation window appears.

8. Click the Unlink button.

   Tenable.io unlinks the agents.
Agent Settings

On your agent's manager, you can configure system-wide agent settings to specify agent and blackout window settings for all your linked agents. For more information on creating, modifying, and deleting blackout windows, see Blackout Windows.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inactive Agents</td>
<td>Specifies the number of days an agent can be inactive before the manager unlinks the agent. After the specified number of days, the agent is unlinked, but the corresponding agent data is not removed from the manager. Tenable.io automatically tracks unlinked agents and related data for the number of days specified in this option. You cannot turn off this tracking.</td>
</tr>
<tr>
<td>Unlink agents that have been inactive for $X$ days</td>
<td><strong>Note:</strong> Inactive agents that were automatically unlinked by Tenable.io do <em>not</em> automatically relink if they come back online.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Override Blackout Windows</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Exclude all agents from software updates</td>
<td>When enabled, this option overrides scheduled blackout windows. It prevents agents from receiving software updates at any time. Agents continue to receive plugin updates and perform scheduled scans.</td>
</tr>
</tbody>
</table>
Manage an Agent's Settings

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

In Tenable.io, you can manage agent settings (versions 7.6 and later) on the **Linked Agents** tab. For information on editing similar settings in Nessus or the command line interface, see [Advanced Settings].

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Sensors** tile.

   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. In the left navigation menu, click **Agents**.

   The **Agents** page appears and the **Linked Agents** tab is active.

5. (Optional) Search for a specific agent or **filter** the agents in the table.

6. Do one of the following:

   **To edit a single agent:**
   a. In the agents table, in the row for the agent you want to edit, click the button.

      The **Edit Agent** window appears.

   b. Edit the agent settings:

      | Setting             | Description                                              | Default | Values                        |
      |---------------------|----------------------------------------------------------|---------|-------------------------------|
      | Nessus Agent Log Level | The logging level of the backend.log log file, as indicated by a normal | normal | • normal - Changes the backend.log |
set of log tags that determine what information to include in the log.

If you manually edited `log.json` to set a custom set of log tags for `backend.log`, this setting overwrites that content.

For more information, see [log.json Format](#).

<table>
<thead>
<tr>
<th>logging level</th>
<th>sets log tags to</th>
</tr>
</thead>
<tbody>
<tr>
<td>normal</td>
<td>&quot;log&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;info&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;warn&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;error&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;trace&quot;</td>
</tr>
<tr>
<td>debug</td>
<td>&quot;log&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;info&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;warn&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;error&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;trace&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;debug&quot;</td>
</tr>
<tr>
<td>verbose</td>
<td>&quot;log&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;info&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;warn&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;error&quot;,</td>
</tr>
</tbody>
</table>

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Default</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugin Compilation Performance</td>
<td>Sets plugin compilation performance, which affects CPU usage. Low performance slows down plugin compilation, but reduces the agent's CPU consumption. Setting the performance to medium or high means that plugin compilation completes more quickly, but the agent consumes more CPU. For more information, see <a href="#">Agent CPU Resource Control</a>.</td>
<td>high</td>
<td>low, medium, or high</td>
</tr>
<tr>
<td>Scan Performance</td>
<td>Sets scan performance, which affects CPU usage. Low performance</td>
<td>high</td>
<td>low, medium, or high</td>
</tr>
</tbody>
</table>
slows down scans, but reduces the agent's CPU consumption. Setting the performance to medium or high means that scans complete more quickly, but the agent consumes more CPU. For more information, see Agent CPU Resource Control.

**Note:** This setting is only available for agents version 8.1 or later.

| **Automatic Host-name Update** | When enabled, when the hostname on the endpoint is modified the new hostname will be updated in the agent's manager. This feature is disabled by default to prevent custom agent names from being overridden. | no | yes or no |

| **Nessus Agent Update Plan** | Sets the agent's update plan to determine whether it keeps up to date with GA releases, | Keep up to date with GA releases, | Keep up to date with GA releases,
To edit multiple agents:

a. Do one of the following:
   - In the agents table, select the check box next to each agent you want to edit.
   - In the table header, select the check box to select the entire page.

The action bar appears at the bottom of the page.

Tip: In the action bar, select Select All Pages to select all linked agents.

b. In the action bar, click the button.

The Edit Agents window appears.

c. Edit the agent settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nessus Agent Log Level</strong></td>
<td>The logging level of the backend.log log file, as indicated by a set of log tags that</td>
<td>normal</td>
<td>• normal - Sets log tags to &quot;log&quot;, &quot;info&quot;,</td>
</tr>
</tbody>
</table>
determine what information to include in the log.

If you manually edited log.json to set a custom set of log tags for backend.log, this setting overwrites that content.

For more information, see log.json Format.

<table>
<thead>
<tr>
<th>Plugin Compilation Performance</th>
<th>Sets plugin compilation performance, which affects CPU usage. Low performance slows down plugin compilation, but reduces the agent’s CPU consumption. Setting the performance to medium</th>
<th>high</th>
<th>low, medium, or high</th>
</tr>
</thead>
</table>

- "warn",
- "error",
- "trace"

- debug - Sets log tags to "log", "info", "warn", "error", "trace", "debug"

- verbose - Sets log tags to "log", "info", "warn", "error", "trace", "debug", "verbose"
or high means that plugin compilation completes more quickly, but the agent consumes more CPU. For more information, see Agent CPU Resource Control.

| Scan Performance | Sets scan performance, which affects CPU usage. Low performance slows down scans, but reduces the agent's CPU consumption. Setting the performance to medium or high means that scans complete more quickly, but the agent consumes more CPU. For more information, see Agent CPU Resource Control. | high | low, medium, or high |

Note: This setting is only available for agents version 8.0 or later.
### Automatic Host-name Update

When enabled, when the hostname on the endpoint is modified the new hostname will be updated in the agent's manager. This feature is disabled by default to prevent custom agent names from being overridden.

| Automatic Host-name Update | When enabled, when the hostname on the endpoint is modified the new hostname will be updated in the agent's manager. This feature is disabled by default to prevent custom agent names from being overridden. | no | yes or no |

### Nessus Agent Update Plan

Sets the agent's update plan to determine what version the agent automatically updates to.

**Note:** This setting is only available for agents version 8.1 or later.

| Nessus Agent Update Plan | Sets the agent's update plan to determine what version the agent automatically updates to. | Keep up to date with GA releases | Keep up to date with GA releases, Opt in to Early Access releases, or Delay updates, staying on an older release |

**Click** Save.

Tenable.io saves your settings, and the changes take effect the next time the agent checks in. For online agents, this can take up to 45 minutes.

If necessary for the setting changed, the agents restart the next time they become idle.
Edit Global Agent Settings

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to edit agent settings in Tenable.io.

To edit agent settings in the new interface:

1. In the upper-left corner, click the  button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Sensors** tile.
   
   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. In the left navigation menu, click **Agents**.
   
   The **Agents** page appears and the **Linked Agents** tab is active.

5. Click the **Settings** tab.
   
   The **Settings** page appears.

6. Edit the **settings** as necessary.

7. Click **Save**.
   
   Tenable.io saves your changes.
# Agent Status

Nessus Agents can be in one of the following statuses:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online</td>
<td>The host that contains the Nessus Agent is currently connected and in com-</td>
</tr>
<tr>
<td></td>
<td>munication with Tenable.io.</td>
</tr>
<tr>
<td>Offline</td>
<td>The host that contains the Nessus Agent is currently powered down or not con-</td>
</tr>
<tr>
<td></td>
<td>nected to a network.</td>
</tr>
<tr>
<td>Initializing</td>
<td>The Nessus Agent is in the process of checking in with Tenable.io.</td>
</tr>
</tbody>
</table>
Export Agents

To export agents data in Tenable.io in the new interface:

1. In the upper-left corner, click the button. The left navigation plane appears.

2. In the left navigation plane, click Settings. The Settings page appears.

3. Click the Sensors tile. The Sensors page appears. By default, Nessus Scanners is selected in the left navigation menu and the Cloud Scanners tab is active.

4. In the left navigation menu, click Agents. The Agents page appears and the Linked Agents tab is active.

5. In the upper-right corner, click the button. The Export plane appears and shows the number of agents that will be exported.

6. In the Formats section, select the CSV format.

7. To export agents data in .csv format, click Export. Your browser's download manager appears.

8. Click OK to save the agents.csv file.

The agents.csv file exported from Tenable.io contains the following data:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Name</td>
<td>The name of the agent</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the agent at the time of export. Possible values are unlinked, online, or offline.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IPv4 or IPv6 address of the agent.</td>
</tr>
<tr>
<td><strong>Platform</strong></td>
<td>The platform the agent is installed on.</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td><strong>Groups</strong></td>
<td>The names of any groups the agent belongs to.</td>
</tr>
<tr>
<td><strong>Group IDs</strong></td>
<td>The group IDs of any groups the agent belongs to.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>The version of the agent.</td>
</tr>
<tr>
<td><strong>Last Plugin Update</strong></td>
<td>The date (in ISO-8601 format) the agent's plugin set was last updated.</td>
</tr>
<tr>
<td><strong>Agent ID</strong></td>
<td>The ID of the agent.</td>
</tr>
<tr>
<td><strong>Agent UUID</strong></td>
<td>The UUID of the agent.</td>
</tr>
<tr>
<td><strong>Linked On</strong></td>
<td>The date (in ISO-8601 format) the agent was linked to Tenable.io.</td>
</tr>
<tr>
<td><strong>Last Connect</strong></td>
<td>The date (in ISO-8601 format) of the agent's last check-in.</td>
</tr>
<tr>
<td><strong>Last Scanned</strong></td>
<td>The date (in ISO-8601 format) the agent was last scanned.</td>
</tr>
</tbody>
</table>
## Agent Filters

Tenable.io supports filtering Agents by the following categories:

<table>
<thead>
<tr>
<th>Category</th>
<th>Operator</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distro</td>
<td>contains</td>
<td>In the text box, type the distribution name on which you want to filter.</td>
</tr>
<tr>
<td></td>
<td>does not contain</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>is equal to</td>
<td>In the text box, type the IPv4 or IPv6 addresses on which you want to filter.</td>
</tr>
<tr>
<td></td>
<td>is not equal to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>contains</td>
<td></td>
</tr>
<tr>
<td></td>
<td>does not contain</td>
<td></td>
</tr>
<tr>
<td>Last Connection</td>
<td>earlier than</td>
<td>In the text box, type the date on which you want to filter.</td>
</tr>
<tr>
<td>Last Plugin Update</td>
<td>later than</td>
<td></td>
</tr>
<tr>
<td></td>
<td>on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>not on</td>
<td></td>
</tr>
<tr>
<td>Member of Group</td>
<td>is equal to</td>
<td>From the drop-down list, select from your existing agent groups.</td>
</tr>
<tr>
<td></td>
<td>is not equal to</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>is equal to</td>
<td>In the text box, type the agent name on which you want to filter.</td>
</tr>
<tr>
<td></td>
<td>is not equal to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>contains</td>
<td></td>
</tr>
<tr>
<td></td>
<td>does not contain</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Operator</td>
<td>Value</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Platform</td>
<td>contains / does not contain</td>
<td>In the text box, type the platform name on which you want to filter.</td>
</tr>
<tr>
<td>Status</td>
<td>is equal to / is not equal to</td>
<td>In the drop-down list, select an <a href="#">agent status</a>.</td>
</tr>
<tr>
<td>Version</td>
<td>is equal to / is not equal to / contains / does not contain</td>
<td>In the text box, type the version you want to filter.</td>
</tr>
</tbody>
</table>
Agent Groups

You can use agent groups to organize and manage the agents linked to your Tenable.io. You can add an agent to more than one group, and configure scans to use these groups as targets.

To create and manage agent groups:

- Create an Agent Group
- Edit an Agent Group
- Delete an Agent Group
- Add an Agent to an Agent Group
- Remove an Agent from an Agent Group
- View Agents in an Agent Group
Create an Agent Group

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

You can use agent groups to organize and manage the agents linked to your account. You can add an agent to more than one group and configure scans to use these groups as targets.

Use this procedure to create an agent group in Tenable.io.

To create a new agent group in the new interface:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Sensors** tile.
   
   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. In the left navigation menu, click **Agents**.
   
   The **Agents** page appears and the **Linked Agents** tab is active.

5. Click the **Agent Groups** tab.
   
   The agent groups table appears.

6. In the upper-right corner, click **Add Agent Group**.
   
   The agent group settings plane appears.

7. In the **Group Name** box, type a name for the new agent group.

8. Configure user permissions for the agent group.

9. Click **Save**.
   
   The new agent group appears in the table.

What to do next:
• **Use** the agent group in an agent scan configuration.
Add an Agent to an Agent Group

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to add an agent to an agent group in Tenable.io. You can also add agents to a group when you [modify an agent group](#).

To add an agent to agent groups in the new interface:

1. In the upper-left corner, click the **button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Sensors** tile.
   
   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. In the left navigation menu, click **Agents**.
   
   The **Agents** page appears and the **Linked Agents** tab is active.

5. Click the **Agent Groups** tab.
   
   The **Agent Groups** table appears.

6. (Optional) Search for a specific agent or **filter** the agents in the table. For filter descriptions, see **Agent Filters**.

7. Do one of the following:
   
   - To add a single agent to agent groups:
     
     a. In the agents table, roll over the agent you want to add.

     The action buttons appear in the row.
b. Click the button.

The **Add to Groups** plane appears.

- To add multiple agents to agent groups, do one of the following:
  - In the agents table, select the check box next to each agent you want to add.
  - In the table header, select the check box to select the entire page.

The action bar appears at the bottom of the page.

**Tip:** In the action bar, select **Select All Pages** to select all linked agents.

a. In the action bar, click the button.

The **Add to Groups** plane appears.

8. Do one of the following:

- If there are existing agent groups, select one:
  a. In the search box, search by agent group name.
  b. Click the agent group you want to select.

- If there are no existing agent groups, create one:
  a. Click **add a new group**.

  The agent group settings plane appears.
  
  b. In the text box, type the name of the new group.
  
  c. In the **Users & Groups** section, set the user permissions for the new group.
  
  d. Click **Save**.

  The **Add to Groups** plane reappears. The new group appears in the selection list.

9. Click **Save** to save your changes.

  Tenable.io adds the agent to the selected group or groups.
Edit an Agent Group

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to modify an agent group in Tenable.io.

To modify an agent group in the new interface:

1. In the upper-left corner, click the button.
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   The **Settings** page appears.

3. Click the **Sensors** tile.
   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. In the left navigation menu, click **Agents**.
   The **Agents** page appears and the **Linked Agents** tab is active.

5. Click the **Agent Groups** tab.
   The agent groups table appears.

6. (Optional) Search for a specific agent group or **filter** the agent groups in the table. For filter descriptions, see **Agent Group Filters**.

7. Edit agent group settings:
   a. In the agents table, roll over the agent you want to add.
      The action buttons appear in the row.
   
   b. Click the **edit** button.
      The agent group settings plane appears.
   
   c. In the **Name** box, type a new name for the agent group.
d. Configure user permissions for the agent group.

   e. Click **Save** to save your changes.

       Tenable.io saves your changes.

8. Assign agents to an agent group:

   a. Click the row of the agent group where you want to add agents.

       The agent group details page appears.

   b. Click **Assign Agents**.

       The assign agents page appears.

   c. (Optional) Search for a specific agent or **filter** the agents in the table. For filter descriptions, see **Agent Filters**.

   d. In the agents table, select the check boxes next to the agents you want to add to the agent group.

   e. Click **Assign**.

       Tenable.io adds the agents to the agent group, and the details page appears.
Delete an Agent Group

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to delete an agent group in Tenable.io.

To delete an agent group in the new interface:

1. In the upper-left corner, click the ☐️ button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Sensors** tile.
   
   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. In the left navigation menu, click **Agents**.
   
   The **Agents** page appears and the **Linked Agents** tab is active.

5. Click the **Agent Groups** tab.
   
   The agent groups table appears.

6. (Optional) Search for a specific agent group or **filter** the agent groups in the table. For filter descriptions, see [Agent Group Filters](#).

7. In the row for the agent group that you want to delete, click the 👎 button.
   
   A confirmation window appears.

8. Click **Delete**.
   
   Tenable.io deletes the agent group.
Remove an Agent from an Agent Group

Required Tenable.io Vulnerability Management User Role: Scan Manager or Administrator

Use this procedure to remove an agent or agents from an agent group in Tenable.io.

1. In the upper-left corner, click the button.

The left navigation plane appears.

2. In the left navigation plane, click Settings.

The Settings page appears.

3. Click the Sensors tile.

The Sensors page appears. By default, Nessus Scanners is selected in the left navigation menu and the Cloud Scanners tab is active.

4. Click the Agent Groups tab.

The agent groups table appears.

5. (Optional) Search for a specific agent group or filter the agent groups in the table. For filter descriptions, see Agent Group Filters.

6. In the agent groups table, click the agent group you want to modify.

The Group Details page appears.

7. In the agents table, roll over the agent you want to remove.

The action buttons appear in the row.

8. Click the button.

A confirmation window appears.

9. In the confirmation window, click Remove.

Tenable.io removes the agent or agents from the group.
1. In the upper-left corner, click the ▽ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Sensors** tile.

   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. Click the **Agent Groups** tab.

   The agent groups table appears.

5. In the agent groups table, click the agent group you want to modify.

   The **Group Details** page appears.

6. In the agents table, do one of the following:

   - In the agents table, select the check box next to each agent you want to remove from the group.
   - In the table header, select the check box to select the entire page.

   The action bar appears at the bottom of the page.

   **Tip:** In the action bar, select **Select All Pages** to select all linked agents.

7. In the action bar, click the ▼ button.

   A confirmation window appears.

8. In the confirmation window, click **Remove**.

   Tenable.io removes the agents from the group.
View Agents in an Agent Group

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to view agents in an agent group in Tenable.io.

To view agents in an agent group in the new interface:

1. In the upper-left corner, click the menu button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Sensors** tile.
   
   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. In the left navigation menu, click **Agents**.
   
   The **Agents** page appears and the **Linked Agents** tab is active.

5. Click the **Agent Groups** tab.
   
   The agent groups table appears.

6. (Optional) Search for a specific agent group or filter the agent groups in the table. For filter descriptions, see **Agent Group Filters**.

7. In the agent groups table, click the agent group you want to view.
   
   The **Group Details** page appears. This page contains a table listing the agents assigned to the group.
Agent Group Filters

You can use the filters listed below to filter agent groups in the Agent Groups tab.

<table>
<thead>
<tr>
<th>Category</th>
<th>Operator</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>is equal to</td>
<td>In the text box, type the name of the agent group.</td>
</tr>
<tr>
<td></td>
<td>is not equal to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>contains</td>
<td></td>
</tr>
<tr>
<td></td>
<td>does not contain</td>
<td></td>
</tr>
<tr>
<td>Creation Date</td>
<td>earlier than</td>
<td>In the text box, type the date on which the agent group was created.</td>
</tr>
<tr>
<td></td>
<td>later than</td>
<td></td>
</tr>
<tr>
<td></td>
<td>on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>not on</td>
<td></td>
</tr>
<tr>
<td>Last Modified</td>
<td>earlier than</td>
<td>In the text box, type the date on which the agent group was last modified.</td>
</tr>
<tr>
<td></td>
<td>later than</td>
<td></td>
</tr>
<tr>
<td></td>
<td>on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>not on</td>
<td></td>
</tr>
</tbody>
</table>

Modifications include:

- You modified the agent name or description.
- You added an agent to the group.
- You removed an agent from the group.
Blackout Windows

Blackout windows allow you to schedule times where certain agent activities are suspended for all linked agents. This activity includes:

- Receiving and applying software updates

Blackout windows do not prevent linked agents from:

- Receiving plugin updates
- Installing or executing agent scans

To create and manage blackout windows:

- [Create a Blackout Window](#)
- [Modify a Blackout Window](#)
- [Enable or Disable a Blackout Window](#)
- [Delete a Blackout Window](#)
Create a Blackout Window

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to create blackout windows.

Blackout windows will apply to all linked agents and will prevent the agents from receiving and applying software updates during scheduled windows. Agents will still receive plugin updates and continue performing scheduled scans during these windows.

To create a blackout window for linked agents in the new interface:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Sensors** tile.
   
   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. Click the **Blackout Windows** tab.

5. In the upper-right corner, click the **New Blackout Window** button.
   
   The **New Blackout Window** plane appears.

6. Configure the options as necessary.

7. Click **Save**.
   
   The blackout window is saved and appears on the **Blackout Windows** tab.
Edit a Blackout Window

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to manage a blackout window for agent scanning in Tenable.io.

To edit a blackout window in the new interface:

1. In the upper-left corner, click the ﬁle button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Sensors** tile.

   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. Click the **Blackout Windows** tab.

5. In the blackout window table, click the blackout window you want to modify.

   The **Update a Blackout Window** plane appears.

6. Edit the options as necessary.

7. Click **Save** to save your changes.

   Tenable.io saves the changes to the blackout window.
Enable or Disable a Blackout Window

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to enable or disable a blackout window for linked agents in Tenable.io.

To enable or disable a blackout window for linked agents in the new interface:

1. In the upper-left corner, click the ☰ button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Sensors** tile.
   
   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. Click the **Blackout Windows** tab.

5. Search for the blackout window you want to enable or disable.

6. In the row for the blackout window you want to enable or disable, click the **Status** toggle.
   
   The blackout window is disabled and a confirmation window appears.
Delete a Blackout Window

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to delete a blackout window for agent scanning in Tenable.io.

To delete a blackout window for agent scanning in the new interface:

1. In the upper-left corner, click the ⌁ button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Sensors** tile.
   
   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. Click the **Blackout Windows** tab.

5. Select the blackout windows you want to delete:

   - **Select a single window.**
     
     a. In the blackout windows table, roll over the window you want to delete.
     
     The action buttons appear in the row.

        b. In the row, click the ⚤ button.

        A confirmation window appears.

   - **Select multiple windows.**
     
     a. In the blackout windows table, select the check box next to each window you want to delete.

     The action bar appears at the bottom of the page.
b. In the action bar, click the button.

A confirmation window appears.

6. Click **Delete** to confirm the deletion.

Tenable.io deletes the selected blackout window or windows.
Networks

Note: This section describes the new interface. For information about the classic interface, see [Networks (Classic Interface)](#). For information about navigating the new interface, see [Navigate Tenable.io (New Interface)](#).

In larger enterprises, you can reduce the time and cost of setting up and maintaining locations by deploying environments with the same internal IP addresses. To disambiguate between assets that have the same IP addresses across environments, use networks in Tenable.io.

If you deploy environments with the same internal IP addresses, create a network for each environment you have, and assign scanners and scanner groups to each network. When a scanner scans an asset, the associated network is added to the asset's details. You can filter assets by network or create dynamic tags based on a network. Recast rules and access groups do not support networks.

A scanner or scanner group can only belong to one network at a time.

There are two types of networks:

- **Default network** – The network to which a scanner or scanner group belongs unless you assign it to a custom network.

  You can view scanners in the default network, but you cannot add or remove scanners from the default network.

  If you remove a scanner or scanner group from a custom network, or if you delete a custom network, Tenable.io returns the scanner or scanner groups to the default network.

  Imported scans always belong to the default network.

Note: Assets from Nessus Agents or AWS Pre-Authorized Scanners can only appear in the Default network.

- **Custom network** – A network you create. Add a custom network only if you want to scan targets in separate environments that contain overlapping IP ranges. If your scans do not involve separate environments with overlapping IP ranges, keep all scanners in the Default network.

For more information on networks, see the following topics:
• Create a Network
• View or Edit a Network
• Add a Scanner to a Network
• Remove a Scanner from a Network
• Move Assets to a Network
• Delete Assets in a Network
• Delete a Network
Create a Network

Required Tenable.io Vulnerability Management User Role: Scan Manager or Administrator

Create a custom network only if you want to scan targets in separate environments that contain overlapping IP ranges. If your scans do not involve separate environments with overlapping IP ranges, keep all scanners in the Default network.

To create a new network:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, click Settings.
   
   The Settings page appears.

3. Click the Sensors tile.
   
   The Sensors page appears. By default, Nessus Scanners is selected in the left navigation menu and the Cloud Scanners tab is active.

4. Click the Networks tab.
   
   The Networks page appears.

5. In the upper-right corner, click + Add Network.
   
   The Settings page appears.

6. Type a name for the network.

7. (Optional) Type a description for the network.

8. (Optional) Configure Asset Age Out:

   Note: By default, the Asset Age Out toggle is enabled and the value is set to 180 days. At that point, Tenable.io deletes all asset records and associated vulnerabilities. These cannot be recovered, and the deleted assets no longer count towards your license.
• To change the number of days after which Tenable.io deletes unseen assets, in the **Delete Assets Not Seen in the Last** text box, type the number of days.

• To disable the **Asset Age Out** toggle, click the toggle.

9. In the lower-right corner, click **Create**.

   Tenable.io creates the new network. The **Manage Scanners** page appears.
View or Edit a Network

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

To view or edit the configuration of an existing network:

1. In the upper-left corner, click the **button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Sensors** tile.

   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. Click the **Networks** tab.

   The **Networks** page appears.

5. In the networks table, click the network you want to edit.

   The **Network Details** page appears and the **Settings** tab is active.

6. Edit the name or description of the network. The name can contain any alphanumeric and special characters except `< and >`.

7. Click the **Asset Age Out** toggle to enable or disable the permanent deletion of assets in your network after a specific number of days.

   - In the text box, type the number of days that Tenable.io waits before permanently deleting assets that have not been seen on a scan. The minimum value is 90 and the maximum value is 365.

   **Note:** If you enable this option, Tenable.io immediately deletes assets in the specified network that have not been seen for the specified number of days. All asset records and associated vulnerabilities are deleted and cannot be recovered. The deleted assets no longer count towards your license.
8. Click **Save**.

   Tenable.io saves your changes, and the **Networks** page appears.
Add a Scanner to a Network

Required Tenable.io Vulnerability Management User Role: Scan Manager or Administrator

A scanner or scanner group is part of the default network unless you add it to a custom network. A scanner or scanner group can only be part of one network at a time.

You can only add a scanner group to a custom network if all scanners in that group belong to either the default network or the same custom network. If you try to add a scanner group that contains a scanner already assigned to a different custom network, Tenable.io prevents you from adding the scanner group to the network until you resolve the conflict.

You cannot add an AWS pre-authorized scanner to a network.

Before you begin:

- Create a new network.

  Note: Tenable recommends moving scanners to a new network, rather than an existing network, to prevent unwanted asset merges. If the network where you move a scanner already contains asset records, and the identifiers for assets from the moved scanner match the identifiers already existing in the network, Tenable.io automatically merges those assets.

- If you want to move a scanner from one existing network to another existing network:
  - Note the IP addresses of the assets identified by the scanner you want to move.
  - Use the IP addresses to move the assets from the first network to the second network.
  - Add the scanner from the first network to the second network. Use the steps below to add a scanner.

To add a scanner or scanner group to a network:

1. In the upper-left corner, click the ≡ button.

   The left navigation plane appears.

2. In the left navigation plane, click Settings.

   The Settings page appears.
3. Click the **Sensors** tile.

   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. Click the **Networks** tab.

   The **Networks** page appears.

5. In the networks table, click the network you want to add a scanner or scanner group to.

   The **Settings** page appears.

6. In the left navigation list, click **Manage Scanners**.

   A list of **Available Scanners to Add** and **Member Scanners in Network** appear.

7. In the row of the scanner or scanner group you want to add to the network, click the **+** button.

   Tenable.io determines whether there are any scanner group conflicts:

   If no conflicts are present, Tenable.io adds the scanner or scanner group to the network and moves it to the Member Scanners table.

   If any conflicts are present, Tenable.io displays a message. You need to remove a scanner from the scanner group to resolve the conflict. For more information about removing scanners from scanner groups, see [Edit a Scanner Group](#).

   The scanner or scanner group appears in the **Member Scanners in Network**.
Remove a Scanner from a Network

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

If you remove a scanner or a scanner group from a custom network, Tenable.io reassigns it to the default network.

**Tip:** If you want to delete a scanner group or remove a sensor from a scanner group, see [Delete a Scanner Group](#) and [Remove a Sensor from a Scanner Group](#).

To remove a scanner or scanner group from a network:

1. In the upper-left corner, click the **button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Sensors** tile.

   The **Sensors** page appears. By default, **Nessus Scanners** is selected in the left navigation menu and the **Cloud Scanners** tab is active.

4. Click the **Networks** tab.

   The **Networks** page appears.

5. In the networks table, click the network where you want to remove a scanner or scanner group.

   The **Settings** page appears.

6. In the left navigation plane, click **Manage Scanners**.

   A list of **Available Scanners to Add** and **Member Scanners in Network** appear.

7. In the row of the scanner or scanner group you want to remove from the network, click the **button.

   Tenable.io moves the scanner or scanner group to the default network. The scanner or scanner group appears in the **Available Scanners** list.
Move Assets to a Network

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

When a scanner scans assets, the scanner automatically adds the network to which it belongs to the scanned assets' identifying details. However, if you want to change the network assets are assigned to, you can also manually move assets to a network.

**Note:** Move assets to a new network before you run scans on the new network. If you move assets to a network where scans have already run, Tenable.io may create duplicate asset records that count against your license.

To move an asset or assets to a network from the Networks page:

1. In the upper-left corner, click the ☐️ button.
   
   The left navigation plane appears.

2. In the left navigation plane, click Settings.
   
   The Settings page appears.

3. Click the Sensors tile.
   
   The Sensors page appears. By default, Nessus Scanners is selected in the left navigation menu and the Cloud Scanners tab is active.

4. Click the Networks tab.
   
   The Networks page appears.

5. In the networks table, roll over the network you want to move an asset or assets to.
   
   The action buttons appear in the row.

6. Click the button.
   
   The Move Assets page appears.

7. In the Source Network drop-down box, select the network you want to move an asset or assets to.
8. In the text box, do one of the following:

- To search for a single asset, enter an IP address.
- To search for multiple assets, enter a CIDR range or individual IP addresses separated by commas.

Tenable.io displays the asset or assets that matches your search criteria.

9. Do one of the following:

- **Move a single asset:**
  
  a. In the assets table, roll over the asset you want to move.
  
     The action buttons appear in the row.
  
  b. In the row, click the button.

     Tenable.io moves the asset to the selected network.

- **Move selected assets:**
  
  a. For each asset you want to select, roll over the icon.

     The check box for the asset appears.
  
  b. Click the check box.

     The action bar appears at the bottom of the page.
  
  c. In the action bar, click the button.

     Tenable.io moves the selected asset or assets from the source network to the destination network.

- **Move all assets on the current page:**
  
  a. In the assets table header, click the check box.

     Tenable.io selects all assets on the current page. The action bar appears at the bottom of the page.
  
  b. In the action bar, click the button.
Tenable.io moves the selected assets from the source network to the destination network.

- **Move all assets in the source network:**
  a. Roll over the 🔄 icon of an asset.
    
    The action bar appears at the bottom of the page.
  b. In the action bar, click **Select All Assets**.
    
    Tenable.io selects all assets in the source network.
  c. In the action bar, click the 🔄 button.
    
    Tenable.io moves all assets from the source network to the destination network.

To move an asset or multiple assets to a network from the asset table:

1. In the upper-left corner, click the ⌘ button.
   
   The left navigation plane appears.
2. In the left navigation bar, click **Assets**.
   
   The **Assets** dashboard appears, and displays the assets table.
3. (Optional) Refine the table data. For more information, see **Tenable.io Tables**.
4. (Optional) **Apply** a saved search filter.
5. Do one of the following:

   - **Move a single asset:**
     a. Roll over the asset you want to move.
       
       The action buttons appear in the row.
     b. Click the ➔ button.
     c. The **Move** plane appears.
     d. In the **Default** drop-down box, select the network you want to move the asset to.
e. Click the **Move** button.

f. Tenable.io moves the asset to the selected network.

- **To move selected assets:**
  a. For each asset you want to move, click the check box in the asset row.

  The action bar appears at the bottom of the page.

  b. In the action bar, click the ➔ button.

  The **Move** plane appears.

  c. In the **Default** drop-down box, select the network you want to move the asset to.

  d. Click the **Move** button.

  Tenable.io moves the assets to the selected network.

- **To move all assets on the current page:**
  a. Click the check box in the table header.

  The action bar appears at the bottom of the page.

  b. In the action bar, click the ➔ button.

  The **Move** plane appears.

  c. In the **Default** drop-down box, select the network you want to move the asset to.

  d. Click the **Move** button.

  Tenable.io moves the assets to the selected network.

- **To move all assets:**
  a. Click the check box in the table header.

  b. The action bar appears at the bottom of the page.

  c. In the action bar, click **Select All Assets**.
Note: If you click **Select All Assets**, all assets on the current page and any additional pages will be selected.

d. In the action bar, click **Move**.

e. The **Move** plane appears.

f. In the **Default** drop-down box, select the network you want to move the assets to.

g. Click the **Move** button.

h. Tenable.io moves the assets to the selected network.

Note: Depending on the filter applied and the number of assets selected, it may take some time for Tenable.io to move all assets to the destination network.
Delete Assets in a Network

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

**Tip:** If you want to remove an asset from a network but not delete the asset, see [Move Assets to a Network](#).
Delete Assets Manually

If you manually delete an asset, Tenable.io no longer displays the asset in the default view of the assets table, deletes vulnerability data associated with the asset, and stops matching scan results to the asset. Manually deleted assets continue to count against your Tenable.io license until the assets age out after 90 days.

To view manually deleted assets, see View Deleted Assets.

To delete assets manually:

- Delete an individual asset. For more information, see Delete Assets.
- Delete multiple assets in a network in the classic interface. For more information, see Delete Assets from a Network (Classic Interface).
- Delete multiple assets using the Tenable.io API. For more information, see the Tenable Developer Portal.
Delete Assets Automatically

If you automatically delete assets in a network, Tenable.io permanently deletes the asset and all associated vulnerability data after a specified number of days. Automatically deleted assets do not count against your Tenable.io license.

To automatically delete assets, enable the **Asset Age Out** feature when you create or edit the network.
Delete a Network

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

- If you delete a network, assets that were in the deleted network still retain the network attribute.
- Tenable.io retains any asset records for the deleted network until the assets age out of your licensed assets count. You can still filter for assets that use the deleted network.
- You cannot create a new network that has the same name as a deleted network.

**Before you begin:**

Before you delete a network, consider the following:

- Consider moving assets to a different network before you delete the network. To move assets from a deleted network to another network, you must use the Tenable.io API.
- Tenable.io re-assigns any scanners or scanner groups in the deleted network to the default network. If you want to delete the scanners or scanner groups, see Remove a Sensor from a Scanner Group and Delete a Scanner Group.

**To delete a network:**

1. In the upper-left corner, click the **button.

   The left navigation plane appears.

2. In the left navigation plane, click Settings.

   The Settings page appears.

3. Click the Sensors tile.

   The Sensors page appears. By default, Nessus Scanners is selected in the left navigation menu and the Cloud Scanners tab is active.

4. Click the Networks tab.

   The Networks page appears.
5. In the row of the network you want to delete, click the button.
    A confirmation window appears.

6. Click **Delete**.

    Tenable.io deletes the network.
Connectors

Tenable.io uses connectors, including third-party data connectors, to import assets from other platforms. Tenable.io supports connectors for Vulnerability Management and Container Security.

Vulnerability Management Connectors

Vulnerability Management includes connectors for AWS, GCP, and Microsoft Azure. To use Tenable.io connectors to scan your assets, you must first configure the platform the connector integrates with, then create the connector, as described in the appropriate section for your platform:

- Amazon Web Service (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

After you configure platforms and create connectors, you can manage connectors from the Settings page in Tenable.io.

Note: When using cloud connectors. Tenable recommends allowlisting the IP addresses for the region in which the Tenable.io site resides.

The licensing implications are as follows:

- Assets discovered through the connectors do not count against the license until and unless the asset is scanned for vulnerabilities. Discovery through the connector is free.

- Assets discovered through the connectors that did become licensed fall off the license the day after the asset was terminated. This event can be observed via the connector.

- When an asset is deleted or terminated, Tenable.io deletes the asset's vulnerability data and stops matching scan results to the asset. The asset is also deleted from the default view of the assets table.

Note: Tenable.io does not delete the asset from the Assets table.

Container Security Connectors
For information about Tenable.io Container Security connectors, see Configure CS Connectors to Import and Scan Images.
Amazon Web Services Connector

The Amazon Web Services (AWS) connector provides real-time visibility and inventory of EC2 instances in your AWS account.

To import and analyze information about EC2 instances in AWS, you must first configure AWS to support your connector configuration, then create an AWS connector in Tenable.io.

You can create an AWS connector to discover AWS assets and import them to Tenable.io. Assets discovered through the connectors do not count against the license until and unless the asset is scanned for vulnerabilities.

To assess AWS assets for vulnerabilities, Tenable recommends that you use Frictionless Assessment to assess for vulnerabilities in the cloud. Alternatively, you can run a Nessus scanner or agent scan, which runs plugins locally on the host.

<table>
<thead>
<tr>
<th>Goal</th>
<th>Connector type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Discover AWS assets and assess for vulnerabilities using Frictionless Assessment</strong></td>
<td>• Keyless authentication with Frictionless Assessment enabled</td>
</tr>
<tr>
<td>The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.</td>
<td></td>
</tr>
<tr>
<td>The cloud connector discovers AWS assets and collects an inventory of data points on your AWS EC2 instances, then assesses the hosts for vulnerabilities in the cloud, rather than running plugins locally on the host.</td>
<td></td>
</tr>
<tr>
<td>For more information, see <a href="#">Frictionless Assessment for AWS</a>.</td>
<td></td>
</tr>
<tr>
<td><strong>Discover AWS assets</strong></td>
<td>• Keyless authentication (recommended)</td>
</tr>
<tr>
<td>The cloud connector discovers AWS assets without assessing them for vulnerabilities. Optionally, you can scan discovered assets later using a Nessus scanner or agent scan.</td>
<td>• Key-based authentication</td>
</tr>
<tr>
<td>For more information, see <a href="#">AWS Cloud Connector (Discovery Only)</a>.</td>
<td></td>
</tr>
</tbody>
</table>
To manage existing AWS connectors, see Manage Connectors.

Tip: For descriptions of common connector errors, see Connectors in the Tenable Developer Portal.
Frictionless Assessment for AWS

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

With Frictionless Assessment, Tenable.io discovers and collects an inventory of data points on your AWS EC2 instances. Then, for EC2 instances with an AWS tag that you specify for Frictionless Assessment, Tenable.io assesses the hosts for vulnerabilities in the cloud, rather than running plugins locally on the hosts.

Frictionless Assessment leverages the AWS Systems Manager Inventory and AWS Systems Manager Agent (SSM Agent) to collect the required data. For more information on AWS configuration requirements, see Configure AWS for Frictionless Assessment.

You do not need to configure scanners, Nessus Agents, scans, or scan schedules to assess hosts with Frictionless Assessment.

Operating System Coverage

Frictionless Assessment has vulnerability coverage for EC2 instances created from the following Amazon Machine Images:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Coverage Start Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat</td>
<td>2010-11-10</td>
</tr>
<tr>
<td>Amazon Linux 1 / 2</td>
<td>2020-01-15</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>2020-03-26</td>
</tr>
<tr>
<td>CentOS 6 / 7</td>
<td>2020-01-01</td>
</tr>
</tbody>
</table>

Licensing Considerations
In general in Tenable.io, assets count towards your license as soon as they are assessed for vulnerabilities. Therefore, EC2 hosts that are assessed by Frictionless Assessment count against your license. For more information, see Vulnerability Management Licenses.

When you select AWS tags for hosts to be assessed by Frictionless Assessment, be aware that all hosts with any of those tags will count towards your license. Hosts that are only discovered by the connector, and not assessed by Frictionless Assessment (for example, hosts that do not have a tag you selected for Frictionless Assessment), do not count towards your license.

Limitations

- Frictionless Assessment does not run informational plugins, run remote vulnerability plugins, or gather compliance data.
- A connector configured with Frictionless Assessment only supports one AWS account. If you want to assess hosts across multiple AWS accounts, you must configure a separate connector for each AWS account.
- You must use a single AWS tag key to identify the assets you want Frictionless Assessment to access.
- Tenable.io creates an AWS Systems Manager inventory association on your instance to collect inventory for Frictionless Assessment. However, AWS Systems Manager has a restriction that only one inventory association can be applied to an instance at a time, as described in the AWS Documentation. If you have an existing inventory association applied to your instance, remove it before configuring Frictionless Assessment. For more information, see the AWS Documentation.

Get Started

1. Determine who in your organization has the appropriate AWS credentials to access the AWS console.

2. Depending on who has the AWS credentials, do one of the following:
• If you are setting up the Tenable.io cloud connector and also have the appropriate AWS credentials for your organization:
  a. Ensure your AWS configuration meets the requirements for Frictionless Assessment, as described in Configure AWS for Frictionless Assessment.
  b. Create your AWS connector, as described in Create an AWS Connector with Keyless Authentication for Frictionless Assessment.

• If you are setting up the Tenable.io cloud connector, but someone other than you in your organization has the necessary AWS credentials:
  a. The person with AWS credentials must ensure the AWS configuration meets the requirements for Frictionless Assessment, as described in Configure AWS for Frictionless Assessment.
  b. The person with AWS credentials must manually configure AWS roles and policies for use with Frictionless Assessment.
  c. Create your AWS connector, as described in Create an AWS Connector with Keyless Authentication for Frictionless Assessment.

3. To delete an AWS cloud connector, see Delete a Connector.

4. If you delete a connector, manually delete the CloudFormation stack in AWS, as described in Manually Delete Connector Artifacts in AWS.
Configure AWS for Frictionless Assessment

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Frictionless Assessment leverages the AWS Systems Manager Inventory and AWS Systems Manager Agent (SSM Agent) to collect data from a host and create an inventory of data points on your AWS EC2 instances. You do not need to configure scanners, Nessus Agents, scans, or scan schedules to assess hosts with Frictionless Assessment.

If you have access to your organization’s AWS console, ensure your AWS configuration meets the following requirements before creating the Tenable.io cloud connector.

If someone other than you has access to your organization’s AWS console, ensure they configure AWS to meet the following requirements before you create the Tenable.io cloud connector.

To configure your AWS environment for use with Frictionless Assessment:

1. Set up AWS Systems Manager for your account, as described in the [AWS Systems Manager documentation](#).

2. Ensure that you have access to AWS Systems Manager Inventory. For more information, see [AWS Systems Manager Inventory](#) in the [AWS Systems Manager documentation](#).

3. Ensure your EC2 instances have the SSM Agent installed.
   - Most EC2 instance distributions come with SSM Agent preinstalled. For more information, see [About SSM Agent](#) in the [AWS Systems Manager documentation](#).
   - If your distribution does not have SSM installed, manually install the SSM Agent as described in the [AWS Systems Manager documentation](#).

4. Ensure the target EC2 instances you want to assess with Frictionless Assessment are tagged with a single AWS tag key. For example, you can use the tag key `Tenable`.
   Later, you will select this AWS tag key to identify instances you want to assess with Frictionless Assessment.

5. Tenable.io creates an AWS Systems Manager inventory association on your instance to collect inventory for Frictionless Assessment. However, AWS Systems Manager has a restriction
that only one inventory association can be applied to an instance at a time, as described in the AWS Documentation. If you have an existing inventory association applied to your instance, remove it before configuring Frictionless Assessment. For more information, see the AWS Documentation.

What to do next:

• Depending on who has the AWS credentials for your organization, do one of the following:

  • If you are setting up the Tenable.io cloud connector and also have the appropriate AWS credentials for your organization:
    
    • Create your AWS connector, as described in Create an AWS Connector with Keyless Authentication for Frictionless Assessment.

  • If you are setting up the Tenable.io cloud connector, but someone other than you in your organization has the necessary AWS credentials:
    
    a. Work with the other member in your organization to Manually Configure AWS Roles and Policies for Frictionless Assessment.

    b. Create your AWS connector, as described in Create an AWS Connector with Keyless Authentication for Frictionless Assessment.
Manually Configure AWS Roles and Policies for Frictionless Assessment

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

For a list of requirements that your AWS configuration must meet to use Frictionless Assessment, see Configure AWS for Frictionless Assessment.

When you configure an AWS cloud connector with keyless authentication, Tenable.io uses a Cloud Formation Template to automatically configure the required roles and policies for your AWS account. However, if you cannot use the Cloud Formation Template because someone other than you has access to your organization's AWS credentials, you must manually configure AWS roles and policies to work with Frictionless Assessment.

You can manually configure AWS to work with Frictionless Assessment in one of two ways:

**Option 1:** Give Cloud Formation Template to another member of your organization

1. In the AWS console, log in to any AWS account. The account does not need to be the account you want to set up on the connector.
2. In the same browser, log in to Tenable.io.
3. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

4. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

5. Click the **Cloud Connectors** tile.

   The **Connectors** page appears. By default, the **Connectors** page displays a table of configured connectors.

6. In the upper-right corner of the page, click the **Create Connector** button.

   The **Select a Connector** plane appears.
7. In the **Connectors** section, click **AWS - Keyless setup**.

   The **Set up Tenable Frictionless Assessment and Cloud Connector** settings plane appears.

8. Click **Create Stack**.

   Another window or tab in your browser directs you to create a stack in AWS.

   Even though you are not logged into the AWS account you want to set up on the connector, the Cloud Formation Template .yml file is still valid and is specific to your instance of Tenable.io.

9. On the AWS stack creation page, under **Template URL**, copy your .yml file address.

10. Provide the address you copied to the member of your organization who has access to the AWS account you want to set up on the connector. They should set up the Cloud Formation Template to create a stack on the account before you create the Tenable.io cloud connector.

**Option 2: Member of your organization with access to AWS account manually sets up roles and permissions in AWS**

Give the following instructions to the member of your organization who has access to the AWS account you want to set up on the connector.

1. Enable CloudTrail and **create a trail** if one does not already exist.

   **Note:** You must turn on All or Write Only Management Events, as well as logging for the trail.

2. Obtain your Tenable.io container ID, as described in [View Information about Your Tenable.io Instance](#).

3. In your AWS account, create a role named **tenableio-connector** to delegate permissions to an IAM user, as described in the [Amazon AWS documentation](#).

   a. In the navigation pane of the console, click **Roles > Create role**.

   b. For role type, click **Another AWS account**.

   c. For **Account ID**, type the ID 012615275169.

      **Note:** 012615275169 is the account ID of the Tenable AWS account that you will be establishing a trust relationship with to support AWS role delegation (keyless authentication).

   d. Select the **Require external ID** checkbox, and type the Tenable.io container ID.
e. Click **Next: Permissions**.

f. Create or reuse a policy with the following permissions:

<table>
<thead>
<tr>
<th>AWS Service</th>
<th>Permission</th>
</tr>
</thead>
</table>
| Amazon EC2    | • DescribeInstances  
|               | • DescribeRegions   |
| AWS CloudTrail| • DescribeTrails    
|               | • GetEventSelectors |
|               | • GetTrailStatus    |
|               | • LookupEvents      |
| Organizations | • ListAccounts      |
| SSM           | • CreateDocument    |
|               | • UpdateDocument    |
|               | • DeleteDocument    |
|               | • CreateAssociation|
|               | • UpdateAssociation|
|               | • DescribeAssociation|
|               | • ListAssociations  |
|               | • DeleteAssociation |
|               | • CreateResourceDataSync|
|               | • UpdateResourceDataSync|
|               | • DeleteResourceDataSync|
| IAM           | • PutRolePolicy    |
• GetRolePolicy

**Note:** Restrict the permissions to the tenableio-connector IAM role using the following:

```
arn:aws:iam::*:role/tenableio-connector
```

Tenable recommends that you set **Amazon Resource Name** to *(all resources)* for each AWS Service.

g. Click **Next: Tagging**.

h. (Optional) Add any desired tags.

i. Click **Next: Review**.

j. In the **Role name** box, type **tenableio-connector**.

**Caution:** The role must be named **tenableio-connector** for the connector to work.

k. Review the role, ensuring that the role name is **tenableio-connector**, and then click **Create role**.

What to do next:

• [Create an AWS Connector with Keyless Authentication for Frictionless Assessment](#)
Create an AWS Connector with Keyless Authentication for Frictionless Assessment

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

When you configure an AWS cloud connector with keyless authentication for Frictionless Assessment, Tenable.io uses a Cloud Formation Template to automatically configure the required roles and policies for your AWS account. This configuration sets up the regular cloud connector as well as Frictionless Assessment.

To use Frictionless Assessment with your AWS connector, you must enter an AWS tag key to identify hosts to be assessed by Frictionless Assessment. If you do not enter a tag key, the connector functions as discovery-only and assets are not assessed for vulnerabilities.

If you do not want to or cannot use the Cloud Formation Template (for example, if someone else in your organization has the AWS credentials), manually configure the necessary permissions for the connector with Frictionless Assessment, as described in [Manually Configure AWS Roles and Policies for Frictionless Assessment](#).

You must create a separate cloud connector for each AWS account that owns hosts you want to evaluate for Frictionless Assessment.

Before you begin:

- Ensure that your AWS configuration meets the requirements for keyless authentication and Frictionless Assessment, as described in [Configure AWS for Frictionless Assessment](#).
- Ensure that you have your organization's AWS credentials, which are required for the automatic stack creation. If someone other than you in your organization has the necessary AWS credentials, give them the appropriate information so they can [manually configure the AWS roles and policies](#) required for Frictionless Assessment.
- For best results, ensure that this is a new AWS cloud connector setup. If you have existing AWS cloud connectors configured, delete the existing `tenableio-connector` IAM role before...
creating the new AWS cloud connector.

- In another window or tab of the same browser with which you are accessing Tenable.io, log in to the AWS console with the AWS account that you want to target with Frictionless Assessment.

To create an AWS connector using keyless authentication for Frictionless Assessment:

1. In the upper-left corner, click the button.
   The left navigation plane appears.
2. In the left navigation plane, click Settings.
   The Settings page appears.
3. Click the Cloud Connectors tile.
   The Cloud Connectors page appears and displays the configured connectors table.
4. In the upper-right corner of the page, click the Create Cloud Connector button.
   The cloud connector selection plane appears.
5. In the Cloud Connectors section, click AWS - Keyless setup.
   The connector creation plane appears.
6. In the Connector Name box, type a name to identify the connector.
7. In the Account ID box, type your primary AWS account ID.

Note: In another window or tab of the same browser, ensure you are logged into the AWS console with the same AWS account information.

8. Click Create Stack to create a stack in your AWS account.

Another window or tab in your browser opens where you can create a stack in AWS. The stack creation is automatically populated with all the required parameters, policies, and roles required for using the Tenable.io connector with Frictionless Assessment.
9. On the AWS stack creation page, do the following:
   
a. (Optional) For **Stack name**, modify the stack name to identify the stack.

b. Under **Capabilities**, select the check box to acknowledge the required IAM resources.

c. Click **Create stack**.

   AWS may take a few minutes to create the stack.

d. Wait and confirm that the stack is created.

10. Navigate back to the window or tab in your browser where you were creating your connector in Tenable.io.

11. Under **Frictionless Assessment**, type the AWS tag associated with the hosts you want to assess with Frictionless Assessment:

   a. In the **Tag Key** box, type the AWS tag key.

      For example, in the AWS tag `Tenable:FA`, the tag key is `Tenable`.

   b. In the **Tag Value** box, do one of the following:

      i. To identify a specific AWS tag, type the AWS tag value.

         For example, in the AWS tag `Tenable:FA`, the tag value is `FA`.

      ii. To use a wildcard to match all AWS tags with the **Tag Key**, leave the **Tag Value** box blank.

         For example, `Tenable:<blank>` would match any AWS tag with the key `Tenable`, such as `Tenable:FA`, `Tenable:true`, and `Tenable:false`.

   **Note:** The tag key and value are case sensitive and must match what is in AWS exactly.

   **Note:** To use Frictionless Assessment with your AWS connector, you must enter an AWS tag key to identify hosts to be assessed by Frictionless Assessment. If you do not enter a tag key, the connector functions as discovery-only and assets are not assessed for vulnerabilities.
12. (Optional) To modify more advanced Tenable.io cloud connector settings, click **Cloud Connector Advanced Settings** to expand the settings.

   a. (Optional) Use the **Auto Discovery** toggle to enable or disable automatic discovery of linked accounts and CloudTrails.

   b. (Optional) If you disabled **Auto Discovery**, do any of the following:
      
      - To manually add AWS accounts, next to **Accounts for Cloud Assessment**, click +.
      
      - To manually add AWS CloudTrails, next to **AWS CloudTrails for Cloud Assessment**, click +.

   c. (Optional) In the **Select or Create Network** drop-down box, select an existing network to which the connector should be added.

   When the connector discovers an asset, the associated network is added to the asset's details. For more information, see **Networks**.

   d. (Optional) Use the **Cloud Connector Schedule** toggle to enable or disable scheduled imports.

   **Note:** Updates to AWS tags only sync with Tenable.io when the connector imports data from AWS. If you disable the automatic import schedule, you must **import manually** to update your Frictionless Assessment tags and assets.

   By default, Tenable.io requests new and updated asset records every 1 day.

   If you enable schedule imports:
   
   i. In the text box, type the frequency with which Tenable.io sends data requests to the AWS server.
   
   ii. In the drop-down box select **Minutes**, **Hours**, or **Days**.

13. Do one of the following:

   - To save the connector, click **Save**.
   
   - To save the connector and import your assets from AWS, click **Save & Import**.
Tenable.io imports your assets from AWS. There may be a short delay before your assets appear.

What to do next:

- [View Assets](#) to see hosts that were discovered by the connector. Hosts found by an AWS connector using Frictionless Assessment appear with the source [SSM](#).

- [View vulnerabilities](#) to see vulnerabilities identified by Frictionless Assessment.
Manually Delete Connector Artifacts in AWS

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

After you delete your last AWS connector with keyless authentication, Tenable.io triggers an automatic deletion of most AWS artifacts associated with the connector and the Frictionless Assessment configuration.

The following artifacts are automatically deleted:

- **Documents** – `TenableInventoryCollection`
- **Associations** – `TenableInventoryAssociation`
- **Resource Data Sync** – Specific to your Tenable.io site. For example, `tenb-inv-upload-us-east-1-us-1a-sync`.

However, the CloudFormation stack and the `tenableio-connector` IAM role are **not** automatically deleted. You must manually delete the CloudFormation stack in the AWS CloudFormation console. When you delete the CloudFormation stack, the IAM role is automatically deleted.

Before you begin:

- Delete the AWS connector, as described in [Delete a Connector](#).

To manually delete artifacts from the AWS connector:

- Delete the Tenable-created CloudFormation stack named `tenableio-connector-aws-keyless-fa-cft`, as described in [Deleting a stack on the AWS CloudFormation console](#) in the [AWS CloudFormation User Guide](#).

  When you delete the CloudFormation stack, the IAM role is automatically deleted.
AWS Cloud Connector (Discovery Only)

The Amazon Web Services (AWS) cloud connector provides real-time visibility and inventory of EC2 assets in AWS accounts.

You can create an AWS connector to discover AWS assets and import them to Tenable.io. Assets discovered through the connectors do not count against the license until and unless the asset is scanned for vulnerabilities.

**Tip:** To configure an AWS connector with Frictionless Assessment, which allows you to assess EC2 instances for vulnerabilities without configuring agents or scans, see [Frictionless Assessment for AWS](#).

You can create AWS connectors for discovery with either of the following configurations:

- **Recommended:** [AWS Connector with Keyless Authentication (Discovery Only)](#)
- [AWS Connector with Key-based Authentication](#)
The Amazon Web Services (AWS) Connector provides real-time visibility and inventory of EC2 assets in AWS accounts.

You can create an AWS connector to discover AWS assets and import them to Tenable.io. Assets discovered through the connectors do not count against the license until and unless the asset is scanned for vulnerabilities.

Tip: To configure an AWS connector with Frictionless Assessment, which allows you to assess EC2 instances for vulnerabilities without configuring agents or scans, see Frictionless Assessment for AWS.

Keyless Authentication

Tenable.io AWS connectors support keyless authentication via AWS role delegation. Keyless authentication via AWS role delegation allows the automatic discovery of your AWS assets. To use keyless authentication, you must establish a trust relationship between your AWS accounts and the Tenable AWS account. In this scenario, your AWS accounts communicate with a trusted Tenable AWS account that communicates with your AWS connector.

Automatic Discovery of AWS Accounts

If you want to allow the Tenable AWS Account to automatically find other AWS accounts in your organization, use keyless authentication with auto discovery. You must enable AWS Organizations and assign a ListAccounts policy, which then discovers other AWS accounts and establishes trust relationships as shown in the following diagram.
Manual Linking of AWS Accounts

If you do not want to use auto discovery or if you are not using AWS Organizations, you can manually configure linked AWS accounts, as shown in the following diagram.
To configure and create an AWS connector with keyless authentication:

1. Configure AWS for Keyless Authentication (Discovery Only)
2. Create an AWS Connector with Keyless Authentication (Discovery Only)
Configure AWS for Keyless Authentication (Discovery Only)

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

Before you create a discovery-only connector with keyless authentication, you must first configure AWS. For more information on linking AWS accounts and establishing trust relationships, see [AWS Connector with Keyless Authentication (Discovery Only)](https://docs.tenable.com/en/security-center/connector/aws-keyless-authentication.html)

Before you begin:

1. On your AWS account, enable CloudTrail.
2. Create a trail if one does not already exist.
3. In the trail, turn on **All** or **Write Only** Management Events, as well as logging.

**Note:** When an AWS connector is used to import assets, Tenable queries all the CloudTrails for that connector and determine the set of all regions that those CloudTrails receive events for. That set of regions is then used when making calls to the EC2 and CloudTrail APIs.

To manually configure AWS for a discovery-only connector with keyless authentication:

1. Obtain your Tenable.io container ID, as described in [View Information about Your Tenable.io Instance](https://docs.tenable.com/en/security-center/connector/aws-keyless-authentication.html).
2. In your AWS account, create a role named `tenableio-connector` to delegate permissions to an IAM user:

   **Tip:** For more information, see the [Amazon AWS documentation](https://docs.aws.amazon.com/iam/latest/dg/access-keys-manage.html).

   a. In the navigation pane of the AWS console, click **Roles > Create role**.
   b. For role type, click **Another AWS account**.
   c. For **Account ID**, type the ID `012615275169`.

   **Note:** `012615275169` is the account ID of the Tenable AWS account that you will be establishing a trust relationship with to support AWS role delegation.
d. Select the **Require external ID** check box, and type the Tenable.io container ID that you obtained in step 1.

e. Click **Next: Permissions**.

f. Create or reuse a policy with the following permissions:

<table>
<thead>
<tr>
<th>AWS Service</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon EC2</td>
<td>• DescribeInstances</td>
</tr>
<tr>
<td>AWS CloudTrail</td>
<td>• DescribeTrails</td>
</tr>
<tr>
<td></td>
<td>• GetEventSelectors</td>
</tr>
<tr>
<td></td>
<td>• GetTrailStatus</td>
</tr>
<tr>
<td></td>
<td>• ListTags</td>
</tr>
<tr>
<td></td>
<td>• LookupEvents</td>
</tr>
<tr>
<td>AWS Organizations</td>
<td>• ListAccounts</td>
</tr>
</tbody>
</table>

**Note:** The `ListAccounts` permission is required for Tenable.io to automatically discover AWS accounts. If you do not use auto discovery, you do not need this permission.

**Note:** Tenable recommends that you set **Amazon Resource Name** to *(all resources)* for each AWS Service

g. Click **Next: Tagging**.

h. (Optional) Add any desired tags.

i. Click **Next: Review**.

j. In the **Role name** box, type *tenableio-connector*.

**Caution:** The role must be named *tenableio-connector* for the connector to work.

k. Review the role, ensuring that the role name is *tenableio-connector*, and then click **Create role**.

What to do next:
• Create an AWS Connector with Keyless Authentication (Discovery Only)
Create an AWS Connector with Keyless Authentication (Discovery Only)

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

You can create an AWS connector to discover AWS assets and import them to Tenable.io. Assets discovered through the connectors do not count against the license until and unless the asset is scanned for vulnerabilities.

Before you begin:

- Configure AWS for Keyless Authentication (Discovery Only)

To create an AWS connector with keyless authentication for discovery only:

1. In the upper-left corner, click the **button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Cloud Connectors** tile.

   The **Cloud Connectors** page appears and displays the configured connectors table.

4. In the upper-right corner of the page, click the **Create Cloud Connector** button.

   The cloud connector selection plane appears.

5. In the **Cloud Connectors** section, click **AWS - Keyless setup**.

   The connector creation plane appears.

6. In the **Connector Name** box, type a name to identify the connector.

7. In the **Account ID** box, type your primary AWS account ID.
**Note:** For discovery-only connectors, skip the stack creation steps in the user interface. The stack configures parameters, policies, and roles required for using the Tenable.io connector with Frictionless Assessment, which includes more permissions than necessary for discovery-only connectors.

8. Skip the **Frictionless Assessment** section.

9. (Optional) To expand more cloud connector settings, click **Cloud Connector Advanced Settings**.
   
   a. (Optional) Use the **Auto Discovery** toggle to enable or disable automatic discovery of linked accounts and CloudTrails.
   
   b. (Optional) If you disabled **Auto Discovery**, do any of the following:
      
      - To manually add AWS accounts, next to **Accounts for Cloud Assessment**, click 
        
      - To manually add AWS CloudTrails, next to **AWS CloudTrails for Cloud Assessment**, click 
        
   c. (Optional) In the **Select or Create Network** drop-down box, select an existing network to which the connector should be added.
      
      When the connector discovers an asset, the associated network is added to the asset’s details. For more information, see [Networks](#).

   d. (Optional) Use the **Cloud Connector Schedule** toggle to enable or disable scheduled imports.
      
      By default, Tenable.io requests new and updated asset records every 1 day.
      
      If enabled:
      
      i. In the text box, type the frequency with which Tenable.io sends data requests to the AWS server.
      
      ii. In the drop-down box select **Minutes, Hours, or Days**.
10. Do one of the following:

   - To save the connector, click **Save**.
   - To save the connector and import your assets from AWS, click **Save & Import**.

   Tenable.io imports your assets from AWS. There may be a short delay before your assets appear.

What to do next:

   - **View Assets** to see assets that were discovered by the connector.
AWS Connector with Key-based Authentication

The Amazon Web Services (AWS) Connector provides real-time visibility and inventory of EC2 assets in AWS accounts.

You can create an AWS connector to discover AWS assets and import them to Tenable.io. Assets discovered through the connectors do not count against the license until and unless the asset is scanned for vulnerabilities.

Key-based Authentication

Tenable.io AWS connectors support key-based authentication that uses an IAM user with permissions and a secret key and access key. In this scenario, the Tenable.io AWS connector authenticates with your primary AWS account via a secret key and an access key. Additionally, you can manually configure secondary linked AWS accounts with trust relationships to your primary AWS account, as shown in the diagram below.

For more information about other AWS authentication options, see Amazon Web Services Connector.

**Note:** AWS connectors configured with key-based authentication do not support the automatic discovery of AWS accounts. Additionally, key-based authentication is not recommended.

To fully configure AWS key-based authentication with Tenable.io:
1. In AWS, configure your primary AWS account to support key-based authentication for your connectors, as described in Configure AWS for Key-based Authentication.

2. (Optional) In AWS, manually configure linked AWS accounts, as described in Configure Linked AWS Accounts (Key-based).

3. In Tenable.io, create your AWS connector, as described in Create an AWS Connector with Key-based Authentication.
Configure AWS for Key-based Authentication

**Required User Role:** Administrator

Before you begin:

- Enable CloudTrail and **create a trail** if one does not already exist.

  **Note:** You must turn on **All** or **Write Only** Management Events, as well as logging for the trail.

To configure AWS to support Tenable.io connectors via an IAM user with permissions (key-based authentication):

1. **Use the Policy Generator to create an IAM permission policy** for integration with Tenable.io.

2. Add the following permissions to the policy:

<table>
<thead>
<tr>
<th>AWS Service</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC2</td>
<td>• DescribeInstances</td>
</tr>
<tr>
<td>CloudTrail</td>
<td>• DescribeTrails</td>
</tr>
<tr>
<td></td>
<td>• GetEventSelectors</td>
</tr>
<tr>
<td></td>
<td>• GetTrailStatus</td>
</tr>
<tr>
<td></td>
<td>• ListTags</td>
</tr>
<tr>
<td></td>
<td>• LookupEvents</td>
</tr>
</tbody>
</table>

Tenable recommends that you set **Amazon Resource Name** to *(all resources)* for each AWS Service.

3. **Create an IAM user with programmatic access.**

4. **Assign the policy you created in Step 2 to the IAM user.**

5. **Obtain Access and Secret keys.**

(Optional) To configure linked AWS accounts:

- **Link AWS Accounts**
What to do next:

- Create an AWS connector with Keyed Authentication.
Configure Linked AWS Accounts for Key-based Authentication

This section assumes that access keys have already been generated for the primary account, and explains how to configure linked AWS accounts as depicted in the diagram below.

Before you begin:

- Configure the primary AWS account.
- Record the Account ID for the primary AWS account.

To configure linked AWS accounts:

1. Obtain your Tenable.io container ID, as described in View Information about Your Tenable.io Instance.

2. In your AWS account, create a role named tenableio-connector to delegate permissions to an IAM user, as described in the Amazon AWS documentation.
   a. In the navigation pane of the console, click Roles > Create role.
   b. For role type, click Another AWS account.
   c. For Account ID, type the AWS account ID of the primary AWS account.
d. Select the **Require external ID** check box, and type the Tenable container ID that you obtained in Step 1.

e. Click **Next: Permissions**.

f. Create or reuse a policy with the following permissions:

<table>
<thead>
<tr>
<th>AWS Service</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon EC2</td>
<td>• DescribeInstances</td>
</tr>
<tr>
<td>AWS CloudTrail</td>
<td>• DescribeTrails</td>
</tr>
<tr>
<td></td>
<td>• GetEventSelectors</td>
</tr>
<tr>
<td></td>
<td>• GetTrailStatus</td>
</tr>
<tr>
<td></td>
<td>• ListTags</td>
</tr>
<tr>
<td></td>
<td>• LookupEvents</td>
</tr>
</tbody>
</table>

Tenable recommends that you set **Amazon Resource Name** to *(all resources)* for each AWS Service.

g. Click **Next: Tagging**.

h. (Optional) Add any desired tags.

i. Click **Next: Review**.

j. In the **Role name** box, type **tenableio-connector**.

   **Caution:** The role *must* be named **tenableio-connector** for the connector to work.

k. Review the role, ensuring that the role name is **tenableio-connector**, and then click **Create role**.

l. Record the **Role ARN** for the created role. You need the Role ARN for the next section of the configuration.

To configure the primary AWS account:

**Note:** For more detailed steps, see the Amazon documentation: [Accessing and Administering the Member Accounts in Your Organization](#).
1. Create a policy that has permission to use the AWS Security Token Service (AWS STS) AssumeRole API (*sts:AssumeRole*) action.
   a. Navigate to Policies and then click Create Policy.
   b. For Service, choose STS.
   c. For Actions, type AssumeRole in the Filter box and then select the check box next to it when it appears.
   d. Click You chose actions that require the role resource type.
   e. Click Add ARN.
   f. In the Specify ARN for role field, paste the ARN recorded for the role created in the linked account(s).
   g. Click Add.
   h. Click Review policy.
   i. In the Name field, type a unique name for your policy.
   j. Click Create Policy.

2. Add the policy created in step 1 to a user or group associated with the access keys used when you created your connector.
   a. Click the Add Permissions button.
   b. Select the Attach existing policies directly check box.
   c. Find the policy with sts:AssumeRole that was created in step 1.
   d. Click Next: Review.
   e. Click Add permissions.
Create an AWS Connector with Key-based Authentication

Required User Role: Administrator

Before you begin:

- Complete the required AWS configuration steps for key-based authentication.

To create an AWS connector:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, click Settings.
   
   The Settings page appears.

3. Click the Cloud Connectors tile.
   
   The Cloud Connectors page appears and displays the configured connectors table.

4. In the upper-right corner of the page, click the Create Cloud Connector button.
   
   The cloud connector selection plane appears.

5. In the Cloud Connectors section, click AWS - Keyed setup.
   
   The cloud connector creation plane appears.

6. In the Connector Name box, type a name to identify the connector.

7. In the Access Key box, type the access key that you obtained when configuring AWS.

8. In the Secret Key box, type the secret key that corresponds to the access key you used.

9. In the Select or Create Network drop-down box, select an existing network for your connector or click the button to create a new network.

Note: Networks help to avoid IP address collisions between cloud assets and Nessus-discovered assets. Tenable recommends creating a network for each connector type in use to prevent asset records in different cloud environments from overwriting each other. For more information about the network feature, see Networks.
10. Use the **Cloud Connector Schedule** toggle to enable or disable scheduled imports.

**Note:** By default, Tenable.io requests new and updated asset records every 1 hour.

If enabled:

- In the **Import** text box, type the frequency with which Tenable.io sends data requests to the AWS server.
- In the drop-down box select *Minutes, Hours, or Days.*

11. Do one of the following:

- To save the connector, click **Save**.
- To save the connector and import your assets from AWS, click **Save & Import**.

**Note:** There may be a short delay before your assets appear in Tenable.io.
The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

The Google Cloud Platform (GCP) Connector provides real-time visibility and inventory of assets in Google Cloud Platform. The GCP connector refreshes according to a schedule set by the user.

To import and analyze information about assets in Google Cloud Platform, you must configure GCP to support connectors and then create a GCP connector in Tenable.io.

To analyze assets via a GCP connector:

1. Configure your GCP account to support your connectors, as described in Configure Google Cloud Platform (GCP).
2. Create your GCP connector, as described in Create a Google Cloud Platform Connector.

**Note:** To manage existing GCP connectors, see Manage Connectors.

**Tip:** For common connector errors, see Connectors in the Tenable Developer Portal.
Configure Google Cloud Platform (GCP)

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

Before you can use Tenable.io GCP connectors, you must configure GCP to support your connectors.

**Note:** Before configuring, you must enable the compute engine API for each project you want scanned from within Google Cloud Platform. See the Google API documentation for more information.

To configure GCP to support Tenable.io connectors:

1. Log into Google Cloud Platform.

2. In the left navigation bar, select IAM & admin.
   
   The IAM & admin page appears.

3. In the **Select a project** drop-down box in the upper-left, select the applicable GCP project.

4. In the left navigation bar, select **Service accounts**.
   
   The Service accounts page for your GCP project appears.

5. Click **CREATE SERVICE ACCOUNT**.
The **Create service account** page appears.

![Create service account page](image)

6. In the **Service account name** box, type a display name for your service account.

7. In the **Service account ID** box, type a unique service account ID.

8. In the **Service account description** box, describe what the service account will do.

9. Click the **CREATE** button.

   The **Grant this service account access to project** page appears.

10. In the drop-down box on the **Service account permissions (optional)** page, add the Logging - > Logs Viewer role.
Note: The service accounts must have the Logging -> Log Viewer role for discovery sync (incremental syncs after initial full sync).

11. Click + ADD ANOTHER ROLE on the Service account permissions (optional) page.

12. Add the Compute Engine -> Compute Viewer role.
13. Click the Continue button.

The Grant users access to this service account page appears.

14. In the Create key (optional) section, click +CREATE KEY.

The create key (optional) pane appears.

15. Under Key type, select JSON to create a key in JSON format.

16. Click the CREATE button.

17. Your browser downloads the key in JSON format.

(Optional) To configure a GCP service account that can access multiple projects:

You may have dozens of GCP accounts that are added and removed regularly. Instead of adding each GCP account as a different connector, you can configure the top-level service account to access multiple projects. The GCP connector automatically discovers all linked projects and pulls assets from those projects.
**Note:** The top-level service account must have the Cloud Resource Manager API enabled in order to access multiple projects.

**Caution:** The GCP connector pulls assets from any project that is configured with access to the top-level service account. Only add projects that you want the GCP connector to pull data from.

2. In the left navigation bar, select **IAM & admin**.
   
The IAM & admin page appears.
3. In the drop-down menu in the upper-left corner, select the second GCP project.
4. In the IAM menu bar, click **+ ADD**.
   
The Add members to project pane appears.
5. In the **New Members** box, type the name of the top-level service account that you created in step 6 of the first section.
6. In the **Select a role** drop-down box, select the appropriate role.
7. (Optional) Click the **+ ADD ANOTHER ROLE** button to add additional roles.
8. To add additional projects, repeat steps 3 through 7.

What to do next:

- Create a GCP Connector, as described in [Create a Google Cloud Platform Connector](https://cloud.google.com).
Create a Google Cloud Platform Connector

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

Before you begin:

- Complete the required GCP configuration steps.

To create a GCP connector:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, click Settings.

   The Settings page appears.

3. Click the Cloud Connectors tile.

   The Cloud Connectors page appears and displays the configured connectors table.

4. In the upper-right corner of the page, click the Create Connector button.

   The Select a Connector pane appears.

5. In the Connectors section, click Google Cloud Platform.

   The Google Cloud Platform pane appears.

6. In the Connector Name: box, type a name to identify the connector.

7. In the Service Account Key section, click Add File to upload your service account key that you obtained when configuring GCP.

8. The Auto Discovery toggle is always enabled and cannot be disabled. Any Project ID(s) associated with the service account you provided are auto-discovered and assets will be pulled from those projects.
9. In the **Select or Create Network** drop-down box, select an existing network for your connector or click the **+** button to create a new network.

   **Note:** Networks help to avoid IP address collisions between cloud assets and Nessus-discovered assets. Tenable recommends creating a network for each connector type in use to prevent asset records in different cloud environments from overwriting each other. For more information about the network feature, see [Networks](#).

10. Use the **Schedule Import** toggle to enable or disable scheduled imports.

   **Note:** By default, Tenable.io requests new and updated asset records every 1 day.

   If enabled:
   - In the **Import** text box, type the frequency with which Tenable.io sends data requests to the GCP server.
   - In the drop-down box select *Minutes, Hours, or Days*.

11. Do one of the following:
   - To save the connector, click **Save**.
   - To save the connector and import your assets from GCP, click **Save & Import**.

   **Note:** There may be a short delay before your assets appear in Tenable.io.
Microsoft Azure Connector

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

The Microsoft Azure Connector provides real-time visibility and inventory of assets in Microsoft Azure accounts. The Azure connector refreshes according to a schedule set by the user.

To import and analyze information about assets in Microsoft Azure, you must configure Azure to support connectors and then create an Azure connector in Tenable.io.

**Note:** If your Azure deployment includes Azure instances in the Azure China or Azure Government regions, Tenable.io cannot connect to those instances.

To analyze assets via a Microsoft Azure connector:

1. Configure your Azure account to support your connectors, as described in [Configure Microsoft Azure](#).

2. Create your Azure connector, as described in [Create a Microsoft Azure Connector](#).

**Note:** To manage existing Microsoft Azure connectors, see [Manage Connectors](#).

**Tip:** For common connector errors, see [Connectors](#) in the Tenable Developer Portal.
Configure Microsoft Azure

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Before you can use Tenable.io Azure connectors, you must perform several steps in Microsoft Azure.

**Note:** If your Azure deployment includes Azure instances in the Azure China or Azure Government regions, Tenable.io cannot connect to those instances.

To configure Microsoft Azure:

1. **Create an Azure Application** if one does not already exist.
   
   **Note:** The Azure Application ID and Client Secret are obtained during this step.

2. **Obtain the Azure Tenant ID (Directory ID).**

3. **Obtain the Azure Subscription ID.**

4. **Grant the Azure Application reader role permissions.**

5. (Optional) **Link Additional Azure Subscriptions to your Azure Application.**

What to do next:

- **Create an Azure connector.**
Create Azure Application

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

To create an Azure Application for an Azure Tenable.io connector:

1. Log in to the Microsoft Azure portal.
2. In the left-hand menu, click **Azure Active Directory**.

3. Click **App registrations**.
4. To add a new application, click **New registration**.
5. In the **Name** box, enter a descriptive name for the application.

6. In the **Supported Account types** section, choose one of the three options to specify the type of accounts that can access the API.

7. (Optional) In the **Redirect URI** section, select either **Web** or **Public client (mobile & desktop)** from the drop-down, and then enter the URI in the text box.

8. Click **Register** to finalize the settings and create the application.

A success message appears at the top of the page stating that the new application has been created, and the page is redirected to the **Overview page** for the application.
9. Copy the **Application (client) ID**. This information is used to configure a connector with Tenable.io.
10. In the **Manage** section for the application, click **Certificates & secrets**.

11. In the **Client Secrets** section, click **+ New client secret**.

12. In the **Description** box, type a description for the client secret.

13. For the **Expires** option, select an expiration date.

14. Click the **Add** button.

   The new client secret is added.

15. Copy or make a note of the client secret value.

   Later, you will need this client secret to configure a connector with Tenable.io.

**What to do next:**

- **Obtain the Azure Tenant ID (Directory ID)**
Obtain Azure Tenant ID (Directory ID)

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

To obtain your Tenant ID for an Azure Tenable.io connector:

1. Log in to the Microsoft Azure portal.
2. In the left-hand menu, click Azure Active Directory.
   - The Directory Overview page appears.
3. In the Manage section, click Properties.
   - The Directory properties page appears.
4. Copy the Directory ID.

Note: The Tenant ID and Directory ID are the same.
What to do next:

- Obtain the Azure Subscription ID.
Obtain Azure Subscription ID

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

To obtain your Subscription ID for an Azure Tenable.io connector:

1. Log in to the Microsoft Azure portal.
2. In the left-hand menu, click All Services.
3. In the **General** section, click **Subscriptions**.

![Subscriptions](image)

4. Copy the **Subscription ID** for the applicable subscription.

What to do next:

- **Grant the Azure Application reader role permissions.**
Grant the Azure Application Reader Role Permissions

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

To grant an Azure application reader role permissions for an Azure Tenable.io connector:

**Note:** For more information, see the Microsoft Azure documentation: [Manage access to Azure resources using RBAC and the Azure portal](#).

1. Log in to the Microsoft Azure portal.
2. In the left-hand menu, click **All Services**.
3. In the **General** section, click **Subscriptions**.

4. In the subscription table, click the applicable subscription.

The **Overview** page for the subscription appears.

5. In the menu for the subscription, click **Access control (IAM)**.

The **Access control (IAM)** page appears.

6. Click the **+Add** button.

A pop-up menu appears.
7. Click **Add role assignment**.
8. In the **Add role assignment** plane, in the **Role** drop-down, select **Reader**.
9. In the Assign access to drop-down, select Azure AD user, group, or service principal.
10. In the **Select** drop-down, select your Azure Application.

11. Click the **Save** button.

**What to do next:**

**Do one of the following:**

- (Optional) **Link Additional Azure Subscriptions to your Azure Application.**
- **Create an Azure connector.**
Link Azure Subscriptions

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Before you begin:

- Record the name of the [application you created](#) for your primary Azure subscription.

To configure linked Azure subscriptions:

Grant the secondary subscription reader role permissions for the application you created for your primary Azure subscription.

1. Log in to the Microsoft Azure portal.
2. In the left-hand menu, click **All Services**.
3. In the **General** section, click **Subscriptions**.

4. In the subscription table, click the applicable subscription.

   The **Overview** page for the subscription appears.

5. In the menu for the subscription, click **Access control (IAM)**.

   The **Access control (IAM)** page appears.

6. Click the **+Add** button.

   A pop-up menu appears.
7. Click **Add role assignment.**
8. In the **Add role assignment** plane, in the **Role** drop-down, select **Reader**.
9. In the **Assign access to** drop-down, select **Azure AD user, group, or service principal**.
10. In the **Select** drop-down, select your Azure Application.

11. Click the **Save** button.

What to do next:

- **Create an Azure connector.**
Create a Microsoft Azure Connector

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

Before you begin:

- Complete the required Microsoft Azure configuration steps.
- Update your plugin set to 2018-12-19 or later.

To create a Microsoft Azure connector:

1. In the upper-left corner, click the button. The left navigation plane appears.
2. In the left navigation plane, click Settings. The Settings page appears.
3. Click the Cloud Connectors tile. The Cloud Connectors page appears and displays the configured connectors table.
4. In the upper-right corner of the page, click the Create Connector button. The Select a Connector plane appears.
5. In the Connecters section, click Microsoft Azure. The Microsoft Azure settings plane appears.
6. In the Connector Name box, type a name to identify the connector.
7. In the Application ID box, type the Azure application ID that you obtained when configuring Microsoft Azure.
8. In the Tenant ID box, type the Azure Tenant ID obtained when configuring Microsoft Azure.
9. In the Client Secret box, type the client secret obtained when configuring Microsoft Azure.
10. Use the **Auto Discovery** toggle to enable or disable automatic discovery of Azure subscription ID(s).

**Note:** Auto discovery is enabled by default. The Azure connector automatically discovers your subscription ID and any linked subscription ID(s).

11. (Optional) If **Auto Discovery** is disabled, manually add one or more subscription IDs:

a. In the **Subscription IDs** section, click the **+** button next to **Subscription IDs**.

   The **Add Subscription IDs** plane appears.

b. In the **Subscription ID** box, type the subscription ID obtained when configuring Microsoft Azure.

c. (Optional) Click the **+** button next to **Add Another Subscription ID** to add additional linked Azure accounts.

d. In the **Subscription ID** box, type the subscription ID for the Azure account that you want to link. For information about configuring linked subscriptions, see [Link Azure Subscription](#).

e. To add the Subscription ID(s), click **Add**.

   Tenable.io displays the **Microsoft Azure** settings plane, and the Subscription ID(s) you linked are listed under **Subscription IDs**.

12. In the **Select or Create Network** drop-down box, select an existing network for your connector or click the **+** button to create a new network.

**Note:** Networks help to avoid IP address collisions between cloud assets and Nessus-discovered assets. Tenable recommends creating a network for each connector type in use to prevent asset records in different cloud environments from overwriting each other. For more information about the network feature, see [Networks](#).

13. Use the **Schedule Import** toggle to enable or disable scheduled imports.

**Note:** By default, Tenable.io requests new and updated asset records every (1) days.

When enabled:
• In the **Import** text box, type the frequency with which Tenable.io sends data requests to the Azure server.

• In the drop-down box select **Minutes**, **Hours**, or **Days**.

14. Do one of the following:

• To save the connector, click **Save**.

• To save the connector and import your assets from Azure, click **Save & Import**.

**Note:** There may be a short delay before your assets appear in Tenable.io.
Launch a Connector Import Manually

**Required User Role:** Administrator

To launch a manual import for a connector:

1. In the upper-left corner, click the ➕ button.
   
   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
   The **Settings** page appears.

3. Click the **Cloud Connectors** tile.
   
   The **Cloud Connectors** page appears and displays the configured connectors table.

4. In the connector table, click the [←] button next to the connector from which you want to launch a manual import.

   Tenable.io sends a request for data to the source. During the request processing, the import button appears as a check mark. You cannot launch another manual import for that connector until the request process completes.
Manage Existing Connectors

The **Settings** page displays the **Connectors** table, which lists all your configured connectors. To manage your connectors, see the following:

- **Search** for a connector.
- **View connectors details** for information about your recent connector imports.
- **View connector event history** to troubleshoot issues.
- **Launch a connector import manually** to initiate an on-demand asset import.
- **Edit a connector** to update the connector details or import schedule.
- **Delete a connector** to remove the connector and associated asset sources from your dashboard.
Launch a Connector Import Manually

**Required User Role:** Administrator

To launch a manual import for a connector:

1. In the upper-left corner, click the  button.
   
The left navigation plane appears.

2. In the left navigation plane, click **Settings**.
   
The **Settings** page appears.

3. Click the **Cloud Connectors** tile.
   
The **Cloud Connectors** page appears and displays the configured connectors table.

4. In the connector table, click the [← button next to the connector from which you want to launch a manual import.
   
   Tenable.io sends a request for data to the source. During the request processing, the import button appears as a check mark. You cannot launch another manual import for that connector until the request process completes.
View Connectors Details

**Required User Role:** Administrator

On the **Connectors** page, you can view details about your connectors and imports.

**Note:** You can also complete connector management tasks from the **Connectors** page, including launching an import manually, editing a connector, and deleting a connector. For more information, see [*Manage Existing Connectors*](#).

Before you begin:

- Configure the platform your connector must access and create your connector, as described in [*Connectors*](#).

To view connector and import details:

1. In the upper-left corner, click the **[ ]** button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Cloud Connectors** tile.

   The **Cloud Connectors** page appears and displays the configured connectors table.

4. In the **Connectors** table, you can:

   a. Search the **Connectors** table.

   b. View details about your connectors and imports.

<table>
<thead>
<tr>
<th>Column</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>View the name of the connector.</td>
</tr>
<tr>
<td>Type</td>
<td>View the platform or registry type from which your connector pulls assets.</td>
</tr>
</tbody>
</table>
### Status
View the status for your most recent asset import.

**Note**: If your connector is a Tenable.io Container Security connector, you can hover over the connector row in the **STATUS** column to view error details for failed imports.

<table>
<thead>
<tr>
<th>Date Created</th>
<th>View the date your connector was created in MM/DD/YYYY format.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Click the column header to sort your connectors by creation date.</td>
</tr>
</tbody>
</table>

### Last Import
View the date for the most recent asset import.

**Note**: If your connector is a Tenable.io Container Security connector, a green icon appears next the date after the import starts. You can hover over the icon to view details for each asset the connector imports. As the import progresses, the details update in real time.
View Connector Event History

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required User Role:** Administrator

For Microsoft Azure connectors and AWS connectors configured with keyless authentication, you can view connector event history to help you troubleshoot issues. You can see events such as when Tenable.io synced with the connector, imported assets, or checked for terminated assets.

Before you begin:

- Configure the platform your connector must access and create your connector, as described in **Connectors**.

To view connector event history:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Cloud Connectors** tile.

   The **Cloud Connectors** page appears and displays the configured connectors table.

4. In the connector table, click the connector for which you want to view event history.

   **Note:** You can view event history for Microsoft Azure connectors and AWS connectors configured with keyless authentication.

   The connector settings plane appears.

5. Click **View Event History**.

   The connector plane expands and displays the **Connector Event History** table. The table displays events sent by the connector to Tenable.io, such as when Tenable.io synced with the
connector, imported assets, or checked for terminated assets. For information on connector errors, see Connectors as documented in the Tenable Developer Portal.
Edit a Connector

**Required User Role:** Administrator

From the **Settings** page, you can edit your connector details, including the asset import schedule. The steps to edit a connector vary depending on the platform.

Before you begin:

- Configure and create your connector, as described in [Connectors](#).
- Log in to Tenable.io.

To edit a Microsoft Azure connector:

1. In the upper-left corner, click the **button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Cloud Connectors** tile.

   The **Cloud Connectors** page appears and displays the configured connectors table.

4. In the connector table, click the connector that you want to edit.

   The **Edit Connector** pane appears.

5. Modify any of the following connector settings:

   - In the **Select or Create Network** drop-down box, change the existing network for your connector or click the ** button to create a new network.

   - In the **Connector Name** box, change the name of the connector.

   - In the **Application ID** box, change the application ID.

   - In the **Tenant ID** box, change the tenant ID.

   - In the **Client Secret** box, change the client secret.
• Use the **Auto Discovery** toggle to enable or disable automatic discovery of subscription IDs.

• If **Auto Discovery** is disabled, add or remove subscription IDs.

• In the **Schedule Import** options, change the frequency of scheduled imports.

6. Click **Save**.

   Tenable.io saves the connector. There may be a short delay before your assets appear in Tenable.io.

**To edit an Amazon Web Service (AWS) connector:**

1. In the upper-left corner, click the ☐️ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Cloud Connectors** tile.

   The **Cloud Connectors** page appears and displays the configured connectors table.

4. In the connector table, click the connector that you want to edit.

   The **Edit Connector** pane appears.

5. Modify the connector.

**If using AWS role delegation (keyless authentication):**

• In the **Select or Create Network** drop-down box, change the existing network for your connector or click the ✗ button to create a new network.

• In the **Connector Name** box, change the name of the connector.

• Use the **Auto Discovery** toggle to enable or disable automatic discovery of linked accounts and CloudTrails.

• In the **Schedule Import** options, change the frequency of scheduled imports.

**If using key-based authentication:**
• In the **Select or Create Network** drop-down box, change the existing network for your connector or click the + button to create a new network.

• In the **Connector Name** box, change the name of the connector.

• In the **Access Key** box, change the access key.

• In the **Secret Key** box, change the secret key that corresponds to the access key.

• In the **Additional Accounts** section, add or remove linked accounts.

• In the **AWS CloudTrails** section, add or remove CloudTrails.

• Click **Refresh CloudTrails** to query the AWS regions and update the **AWS CloudTrails** table.

• In the **Schedule Import** options, change the frequency of scheduled imports.

6. (Optional) If you selected different trails, click **Find Assets**.

   The number of assets to be imported into Tenable.io appears next to the **Find Assets** button. This number may include assets that were previously imported. No duplicate is created if an asset was previously imported.

7. Click **Save**.

   The connector saves. If you selected different trails, your assets from AWS import. There may be a short delay before your assets appear in Tenable.io.

To edit a Google Cloud Platform (GCP) connector:

1. In the upper-left corner, click the **button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Cloud Connectors** tile.

   The **Cloud Connectors** page appears and displays the configured connectors table.

4. In the connector table, click the connector that you want to edit.
The **Edit Connector** pane appears.

5. Modify any of the following connector settings:
   - In the **Select or Create Network** drop-down box, change the existing network for your connector or click the button to create a new network.
   - In the **Connector Name** box, change the name of the connector.
   - Under **Service Account Key**, click **Add File** to change your service account key.
   - In the **Schedule Import** options, change the frequency of scheduled imports.

6. Click **Save**.

   Tenable.io saves the connector. There may be a short delay before your assets appear in Tenable.io.

### To edit a Tenable.io Container Security connector:


2. In the **Connectors** section of the Container Security dashboard, click **View Connectors**.

   The **Connectors** page appears.

3. In the connector table, click the connector you want to edit.

   The **Enter Connector Details** pane appears.

4. Modify one or more of the following connector details:
   - In the **URL** box, change the URL.
   - In the **PORT** box, change the port ID.
   - In the **USER NAME** box, change your username.
   - In the **PASSWORD** box, change your password.

5. Click **Save**.

   The connector saves. There may be a short delay before your assets appear in Tenable.io.
**Note:** For more information about Tenable.io Container Security connectors, see [Configure Connectors to Import Images](#) in the *Tenable.io Container Security User Guide.*
Delete a Connector

To delete a connector:

1. In the upper-left corner, click the button.
   The left navigation plane appears.
2. In the left navigation plane, click Settings.
   The Settings page appears.
3. Click the Cloud Connectors tile.
   The Cloud Connectors page appears and displays the configured connectors table.
4. In the connector table, click the button next to the connector that you want to delete.
   A Confirm Deletion window appears.
5. Click Delete.
   Tenable.io deletes the connector.

What to do next:

- If you deleted an AWS connector with keyless authentication, see Manually Delete Connector Artifacts in AWS.
You can use specialized Tenable.io pages to analyze vulnerability and asset data in Tenable.io. Some, but not all, analysis pages are available in the new interface. For more information about the interface redesign, see Navigate Tenable.io (New Interface).

To learn more about the primary risk metrics in Tenable.io, see CVSS vs. VPR.

<table>
<thead>
<tr>
<th>Analysis Page</th>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lumin</td>
<td>New</td>
<td>Assess your Cyber Exposure risk. Learn more about your assets, your vulnerabilities, and Tenable-recommended solutions.</td>
</tr>
<tr>
<td>Assets</td>
<td>New or Classic</td>
<td>Learn more about the assets on your network.</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>New or Classic</td>
<td>Learn more about the vulnerabilities impacting your network.</td>
</tr>
<tr>
<td>PCI ASV Workbench</td>
<td>New or Classic</td>
<td>Manage PCI ASV attestation requests.</td>
</tr>
<tr>
<td>Solutions</td>
<td>New</td>
<td>Learn more about Tenable recommended solutions for your vulnerabilities.</td>
</tr>
<tr>
<td>Health Status Workbench</td>
<td>Classic</td>
<td>Learn more about scan and usage data for your Tenable.io deployment.</td>
</tr>
<tr>
<td>Dashboards</td>
<td>New or Classic</td>
<td>View graphical summaries of scans, scan results, and system activity.</td>
</tr>
</tbody>
</table>
Lumin

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Note:** This section describes the new interface. Lumin is not supported in the classic Tenable.io interface.

You can use Tenable Lumin to quickly and accurately assess your Cyber Exposure risk and compare your health and remediation performance to other Tenable customers in your Salesforce industry and the larger population. Lumin correlates raw vulnerability data with asset business criticality and threat context data to support faster, more targeted analysis workflows than traditional vulnerability management tools.

Tenable-provided Cyber Exposure metrics help you quantify your risk to make informed remediation and strategic security decisions. For more information about the metrics used in Lumin analysis, see [Lumin Metrics](#).

To get started with Lumin, see [Get Started with Lumin](#).
Lumin Metrics

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Tenable Lumin uses several metrics to help you assess your Cyber Exposure risk.

- **Cyber Exposure Score (CES)**
- **Vulnerability Priority Rating (VPR)**
- **Asset Criticality Rating (ACR)**
- **Asset Exposure Score (AES)**
- **Assessment Maturity Grade**
- **Remediation Maturity Grade**
- **Tenable Vulnerability Indicator (TVI)**

For information about improving the accuracy of your Lumin metrics and increasing your overall vulnerability management health, see [Improve Your Lumin Metrics](#).

**Cyber Exposure Score (CES)**

Tenable calculates a dynamic CES that represents Cyber Exposure risk as an integer between 0 and 1000, based on the Asset Exposure Score (AES) values for assets scanned in the last 90 days. Higher CES values indicate higher risk.

You can view CES for different groups of assets, including:

- the overall CES for your entire organization (e.g., the CES displayed in the **Cyber Exposure Score** widget)
- the tag-level CES for assets in a specific business context (e.g., the CES displayed in the **Cyber Exposure Score by Business Context/Tag** widget).

<table>
<thead>
<tr>
<th>CES Category</th>
<th>CES Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>650 to 1000</td>
</tr>
<tr>
<td>VPR Category</td>
<td>VPR Range</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Critical</td>
<td>9.0 to 10.0</td>
</tr>
<tr>
<td>High</td>
<td>7.0 to 8.9</td>
</tr>
<tr>
<td>Medium</td>
<td>4.0 to 6.9</td>
</tr>
<tr>
<td>Low</td>
<td>0.1 to 3.9</td>
</tr>
</tbody>
</table>

**Vulnerability Priority Rating (VPR)**

Tenable calculates a dynamic VPR for most vulnerabilities. The VPR is a dynamic companion to the data provided by the vulnerability's CVSS score, since Tenable updates the VPR to reflect the current threat landscape. VPR values range from 0.1-10.0, with a higher value representing a higher likelihood of exploit.

**Note:** Vulnerabilities without CVEs in the National Vulnerability Database (NVD) (e.g., many vulnerabilities with the **Info** severity) do not receive a VPR. Tenable recommends remediating these vulnerabilities according to their CVSS-based severity.

**Note:** You cannot edit VPR values.

Tenable.io provides a VPR value the first time you scan a vulnerability on your network. Then, Tenable.io automatically provides new and updated VPR values daily.

---

**Note:** You can include or exclude assets with predicted scores from your CES. For more information, see [Exclude or Include Assets with Predicted Scores from your CES](#).

To view the CES for your entire organization or for a group of assets, view the widgets on the View the Lumin Dashboard.

For more information about how long Tenable.io takes to calculate or recalculate your CES, see Lumin Data Timing.
Tenable recommends prioritizing vulnerabilities with the highest VPRs that are present on your assets with the highest ACRs.

To view the VPR for a specific vulnerability, view vulnerabilities as described in View Vulnerabilities by Plugin.

VPR Key Drivers

Tenable uses the following key drivers to calculate a vulnerability's VPR.

<table>
<thead>
<tr>
<th>Key Driver</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age of Vuln</td>
<td>The number of days since the National Vulnerability Database (NVD) published the vulnerability.</td>
</tr>
<tr>
<td>CVSSv3 Impact Score</td>
<td>The NVD-provided CVSSv3 impact score for the vulnerability. If the NVD did not provide a score, Tenable.io displays a Tenable-predicted score.</td>
</tr>
<tr>
<td>Exploit Code Maturity</td>
<td>The relative maturity of a possible exploit for the vulnerability based on the existence, sophistication, and prevalence of exploit intelligence from internal and external sources (e.g., Reversinglabs, Exploit-db, Metasploit, etc.). The possible values (High, Functional, PoC, or Unproven) parallel the CVSS Exploit Code Maturity categories.</td>
</tr>
<tr>
<td>Product Coverage</td>
<td>The relative number of unique products affected by the vulnerability: Low, Medium, High, or Very High.</td>
</tr>
<tr>
<td>Threat Sources</td>
<td>A list of all sources (e.g., social media channels, the dark web, etc.) where threat events related to this vulnerability occurred. If the system did not observe a related threat event in the past 28 days, the system displays No recorded events.</td>
</tr>
<tr>
<td>Threat Intensity</td>
<td>The relative intensity based on the number and frequency of recently observed threat events related to this vulnerability: Very Low, Low, Medium, High, or Very High.</td>
</tr>
<tr>
<td>Threat</td>
<td>The number of days (0-730) since a threat event occurred for the vulnerability.</td>
</tr>
</tbody>
</table>

Note: Tenable does not customize these values for your organization; VPR key drivers reflect a vulnerability's global threat landscape.
Recency

Threat Event Examples

Common threat events include:

- An exploit of the vulnerability
- A posting of the vulnerability exploit code in a public repository
- A discussion of the vulnerability in mainstream media
- Security research about the vulnerability
- A discussion of the vulnerability on social media channels
- A discussion of the vulnerability on the dark web and underground
- A discussion of the vulnerability on hacker forums

Asset Criticality Rating (ACR)

Tenable assigns an ACR to each asset on your network to represent the asset's relative criticality as an integer from 1 to 10. A higher ACR indicates higher criticality.

<table>
<thead>
<tr>
<th>ACR Category</th>
<th>ACR Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>9 to 10</td>
</tr>
<tr>
<td>High</td>
<td>7 to 8</td>
</tr>
<tr>
<td>Medium</td>
<td>4 to 6</td>
</tr>
<tr>
<td>Low</td>
<td>1 to 3</td>
</tr>
</tbody>
</table>

Tenable provides an ACR value the first time you scan an asset on your network. Then, Tenable automatically provides new and updated ACR values daily.

**Note:** Tenable recommends reviewing your Tenable-provided ACR values and overriding them, if necessary. You can customize ACR values to reflect the unique infrastructure or needs of your organization, as described in [Edit an ACR](#).

If an asset receives multiple ACR values, Tenable.io prioritizes the values in the following order:

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable,Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
1. If set, the manually overridden ACR value.

2. The Tenable-provided ACR value.

To view the ACR for a specific asset, view the asset details as described in View Asset Details.

ACR Key Drivers

Tenable uses the following key drivers to calculate an asset's Tenable-provided ACR.

<table>
<thead>
<tr>
<th>Key Driver</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>device_type</td>
<td>The device type. For example:</td>
</tr>
<tr>
<td></td>
<td>• <strong>hypervisor</strong> — The device is a Type-1 hypervisor that hosts a virtual machine (e.g., Microsoft Hyper-V, VMware ESX/ESXi, or Xen).</td>
</tr>
<tr>
<td></td>
<td>• <strong>printer</strong> — The device is a networked printer or a printing server.</td>
</tr>
<tr>
<td>device_cap-ability</td>
<td>The device's business purpose. For example:</td>
</tr>
<tr>
<td></td>
<td>• <strong>file_server</strong> — The device is a server that provides file sharing services (e.g., an FTP, SMB, NFS, or NAS server).</td>
</tr>
<tr>
<td></td>
<td>• <strong>mail_server</strong> — The device is a server designated for sending and receiving emails.</td>
</tr>
<tr>
<td>internet_exposure</td>
<td>The device’s location on your network and proximity to the internet. For example:</td>
</tr>
<tr>
<td></td>
<td>• <strong>internal</strong> — The device is located within your local area network (LAN), possibly behind a firewall.</td>
</tr>
<tr>
<td></td>
<td>• <strong>external</strong> — The device is located outside your LAN and not behind a firewall.</td>
</tr>
</tbody>
</table>

Note: Tenable does not customize these values for your organization; ACR key drivers reflect the global threat landscape associated with the asset's characteristics.

Note: Running unauthenticated scans may result in limited or incomplete ACR key drivers.

Asset Exposure Score (AES)
Tenable calculates a dynamic AES for each asset on your network to represent the asset’s relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure.

Tenable calculates AES based on the current ACR (Tenable-provided or custom) and the VPRs associated with the asset.

<table>
<thead>
<tr>
<th>AES Category</th>
<th>AES Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>650 to 1000</td>
</tr>
<tr>
<td>Medium</td>
<td>350 to 649</td>
</tr>
<tr>
<td>Low</td>
<td>0 to 349</td>
</tr>
</tbody>
</table>

To view the AES for a specific asset, see View Assets.

Assessment Maturity Grade

Assessment Maturity provides a high-level summary of how effectively you are scanning for vulnerabilities on your licensed assets. Tenable calculates a dynamic Assessment Maturity grade that represents your assessment scanning health as a letter grade between A and F. An A grade indicates you are assessing your assets frequently and thoroughly.

<table>
<thead>
<tr>
<th>Assessment Maturity Letter Grade</th>
<th>Numerical Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>75 to 100</td>
</tr>
<tr>
<td>B</td>
<td>55 to 74</td>
</tr>
<tr>
<td>C</td>
<td>30 to 54</td>
</tr>
<tr>
<td>D</td>
<td>15 to 29</td>
</tr>
<tr>
<td>F</td>
<td>0 to 14</td>
</tr>
</tbody>
</table>

Your Assessment Maturity grade is the combination of your Assessment Maturity depth grade and your Assessment Maturity frequency grade. Tenable provides an Assessment Maturity grade the first time you scan. Then, Tenable.io automatically provides an updated Assessment Maturity grade daily.

Depth Grade
Tenable calculates your depth grade as the combination of your *scan policy coverage* and *authentication coverage*.

- Scan policy coverage – How many plugins were enabled in your scan policies?
- Authentication coverage – How many of your scans successfully used authentication for full vulnerability detection?

**Tip:** You can configure authentication in [credentialed](https://example.com) scans or [agent](https://example.com) scans.

A high depth grade indicates you are using policies with full plugin coverage and successfully running those plugins on your assets.

<table>
<thead>
<tr>
<th>Depth Grade Letter Grade</th>
<th>Numerical Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>75 to 100</td>
</tr>
<tr>
<td>B</td>
<td>55 to 74</td>
</tr>
<tr>
<td>C</td>
<td>30 to 54</td>
</tr>
<tr>
<td>D</td>
<td>15 to 29</td>
</tr>
<tr>
<td>F</td>
<td>0 to 14</td>
</tr>
</tbody>
</table>

**Frequency Grade**

Tenable calculates your frequency grade based on how often you scan assets on your network. A high frequency grade indicates you are scanning your assets often.

<table>
<thead>
<tr>
<th>Frequency Grade Letter Grade</th>
<th>Numerical Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>75 to 100</td>
</tr>
<tr>
<td>B</td>
<td>55 to 74</td>
</tr>
<tr>
<td>C</td>
<td>30 to 54</td>
</tr>
<tr>
<td>D</td>
<td>15 to 29</td>
</tr>
<tr>
<td>F</td>
<td>0 to 14</td>
</tr>
</tbody>
</table>
To view your Assessment Maturity grade, depth grade, and frequency grade, see View Assessment Maturity Details.

For more information about how long Tenable.io takes to calculate or recalculate your Assessment Maturity grade, see Lumin Data Timing.

Remediation Maturity Grade

Remediation Maturity provides a high-level summary of how effectively you are remediating vulnerabilities on your licensed assets. Tenable calculates a dynamic Remediation Maturity grade that represents your remediation health as a letter grade between A and F. An A grade indicates you are remediating the vulnerabilities on your assets quickly and thoroughly.

<table>
<thead>
<tr>
<th>Remediation Maturity Letter Grade</th>
<th>Numerical Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>75 to 100</td>
</tr>
<tr>
<td>B</td>
<td>55 to 74</td>
</tr>
<tr>
<td>C</td>
<td>30 to 54</td>
</tr>
<tr>
<td>D</td>
<td>15 to 29</td>
</tr>
<tr>
<td>F</td>
<td>0 to 14</td>
</tr>
</tbody>
</table>

Your Remediation Maturity grade is the combination of your Remediation Maturity remediation responsiveness grade and your Remediation Maturity remediation coverage grade. Tenable provides a Remediation Maturity grade the first time you remediate a vulnerability. Then, Lumin automatically provides an updated Remediation Maturity grade daily.

Remediation Responsiveness Grade

Tenable calculates your remediation responsiveness grade as the combination of your average remediation time since discovery and your average remediation time since publication.

- Average remediation time since discovery – How long do you take to remediate a vulnerability after it is first discovered (the **First Seen** date)?
- Average remediation time since publication – How long do you take to remediate a vulnerability after a plugin is first made available (the **Plugin Publication** date)?
A high remediation responsiveness grade indicates you are quickly remediating the vulnerabilities on your assets.

<table>
<thead>
<tr>
<th>Remediation Responsiveness Letter Grade</th>
<th>Numerical Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>75 to 100</td>
</tr>
<tr>
<td>B</td>
<td>55 to 74</td>
</tr>
<tr>
<td>C</td>
<td>30 to 54</td>
</tr>
<tr>
<td>D</td>
<td>15 to 29</td>
</tr>
<tr>
<td>F</td>
<td>0 to 14</td>
</tr>
</tbody>
</table>

**Remediation Coverage Grade**

Tenable calculates your remediation coverage grade as the combination of your *vulnerability remediation percentage* and your *average vulnerabilities per asset*.

- Vulnerability remediation percentage – What percentage of vulnerabilities are remediated on your assets?
- Average vulnerabilities per asset – How many vulnerabilities are discovered on your assets?

A high remediation coverage grade indicates you are remediating a high percentage of the vulnerabilities on your assets.

<table>
<thead>
<tr>
<th>Remediation Coverage Letter Grade</th>
<th>Numerical Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>75 to 100</td>
</tr>
<tr>
<td>B</td>
<td>55 to 74</td>
</tr>
<tr>
<td>C</td>
<td>30 to 54</td>
</tr>
<tr>
<td>D</td>
<td>15 to 29</td>
</tr>
<tr>
<td>F</td>
<td>0 to 14</td>
</tr>
</tbody>
</table>

To view your Remediation Maturity grade, remediation responsiveness grade, and remediation coverage grade, see [View Remediation Maturity Details](#).
For more information about how long Lumin takes to calculate or recalculate your Remediation Maturity grade, see [Lumin Data Timing](#).

### Tenable Vulnerability Indicator (TVI)

Tenable assigns a TVI (TVI-#####-#####) to all unique, publicly disclosed vulnerabilities to uniquely identify an individual vulnerability on your network.

<table>
<thead>
<tr>
<th>Vulnerabilities With TVIs</th>
<th>Vulnerabilities Without TVIs</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Vulnerabilities that are CVE-published</td>
<td>• General security weaknesses (e.g., unsupported software)</td>
</tr>
<tr>
<td>• Vulnerabilities that are not CVE-published</td>
<td>• Vulnerabilities within your in-house, custom applications</td>
</tr>
<tr>
<td>• Vulnerabilities that are covered by Tenable plugins</td>
<td></td>
</tr>
<tr>
<td>• Vulnerabilities that are not covered by Tenable plugins</td>
<td></td>
</tr>
</tbody>
</table>

**Tip:** Tenable.io identifies a vulnerability by CVE, if available. If no CVE is available, Tenable.io displays the TVI. If no TVI is available, Tenable.io displays the plugin ID.
Improve Your Lumin Metrics

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

If you want to improve the accuracy of your Lumin metrics and increase your overall vulnerability management health, evaluate your Tenable-provided values and your scanning strategy.

To improve the accuracy of your Lumin metrics:

1. On the [Assessment Maturity Details](#) page, review your Assessment Maturity grade to evaluate your overall scanning health.

   Do any of the following, depending on what your data shows:
   
   - Perform any actions described in the [Recommended Actions](#) widget.
   - View details about your Assessment Maturity depth grade in the [Depth Grade](#) widget. If necessary, improve your depth grade by increasing the number of plugins enabled in your user-defined templates or scans, or by increasing the number of authenticated or agent scans. For more information, see [Configure Plugins in Vulnerability Management Scans](#), [Credentials in Vulnerability Management Scans](#), or [Tenable-Provided Agent Templates](#).

   Better overall scanning health results in a higher Assessment Maturity score.

   If you improve your Assessment Maturity score, you improve the accuracy of your Tenable-provided ACR and VPR values. Then, more accurate ACR and VPR values improve the accuracy of your AES and CES values.

2. In the [Assets](#) table, review your Tenable-provided ACR values to evaluate the characterizations of the assets on your network. If the ACR values do not reflect the unique infrastructure or needs of your organization, you can override them. For more information, see [Edit an ACR Manually](#).

   More accurate ACR values improve the accuracy of your AES and CES values.

3. On the [Remediation Maturity Details](#) page, review your Remediation Maturity grade to evaluate your overall vulnerability remediation health.

   Do any of the following, depending on what your data shows:
• Perform any actions described in the **Recommended Actions** widget.

• View details about your Remediation Maturity remediation responsiveness grade in the **Remediation Responsiveness Grade** widget. If necessary, improve your remediation responsiveness grade by quickly remediating your most critical (highest VPR) vulnerabilities. For more information, see [View Recommended Actions](#).

• View details about your Remediation Maturity remediation coverage grade in the **Remediation Coverage Grade** widget. If necessary, improve your remediation coverage grade by increasing the number of vulnerabilities you remediate. For more information on the assets with the most critical vulnerabilities, see the **Vulnerability Priority Rating (VPR)** widget described in [Vulnerability Management Overview Dashboard](#).

Better overall remediation health results in a higher Remediation Maturity score.
Edit an ACR Manually

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable Lumin

**Required User Role:** Administrator

You can customize an asset's Asset Criticality Rating (ACR) value to reflect the unique infrastructure or needs of your organization. You can edit the ACR for a single asset independently or multiple assets simultaneously.

**Tip:** Changes to an ACR value (and recalculations for your AES and CES values) take effect within 24 hours.

**Tip:** For information about how Tenable.io prioritizes manually overridden ACR values, see [Asset Criticality Rating (ACR)](#).

**Note:** All Lumin data reflects all assets within the organization's Tenable.io instance.

To edit the ACR for a single asset:

1. Navigate to the new Tenable.io interface, as described in [Access the New Interface](#).
2. In the upper-left corner, click the **button.

   The left navigation plane appears.
3. Do one of the following:

<table>
<thead>
<tr>
<th>Location</th>
<th>Action</th>
</tr>
</thead>
</table>
   | **Asset Details** page | a. In the left navigation plane, in the **Asset View** section, click **Assets**.  
<p>|                 | The <strong>Assets</strong> page appears.                                           |
|                 | b. Click an asset row.                                                 |</p>
<table>
<thead>
<tr>
<th>Assets page</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>In the left navigation plane, in the <strong>Asset View</strong> section, click <strong>Assets</strong>. The <strong>Assets</strong> page appears.</td>
</tr>
<tr>
<td>b.</td>
<td>In the assets table, roll over the asset you want to edit.</td>
</tr>
<tr>
<td>c.</td>
<td>Click the ** 符号 button.</td>
</tr>
<tr>
<td>d.</td>
<td>Click the ** 符号 Edit ACR button. The <strong>Edit Asset Criticality Rating</strong> plane appears.</td>
</tr>
</tbody>
</table>

4. Do one of the following:
   - To modify the ACR value, click or drag the **Asset Criticality Rating** slider to increase or decrease the ACR.
   - To reset an existing ACR value to the Tenable-provided ACR value, click **Reset to Tenable ACR**.

5. (Optional) If you want to include a justification for your ACR change, in the **Overwrite Reasoning** section, select one or more reasons.

   For example, if an asset in your development lab environment received a Tenable-assigned ACR appropriate for a more public asset, you could select **Dev Only** as the overwrite reasoning.

6. (Optional) If you want to include a note about your ACR change, in the **Notes** section, type a note.

7. Click **Save**.

   Tenable.io saves the custom ACR.

To edit the ACR for multiple assets:
1. Navigate to the new Tenable.io interface, as described in Access the New Interface.

2. In the upper-left corner, click the button.

   The left navigation plane appears.

3. In the left navigation plane, click Lumin.

   The Lumin dashboard appears.

4. In the Cyber Exposure Score by Business Context/Tag widget, click the tag for which you want to view asset details.

   The Lumin Business Context/Tag Asset Details page appears, filtered by the tag you selected.

5. Access the Assets page through the Asset Criticality Rating Breakdown widget, the Asset Scan Distribution widget, or the Asset Scan Frequency widget, as described in View Business Context/Tag Asset Details.

   The Assets page appears, filtered by your widget selection.

6. In the table, select the check boxes next to the assets that you want to edit.

   The action bar appears at the bottom of the page.

7. In the action bar, click the button.

   The Lumin Edit Asset Criticality Rating plane appears.

8. Click and drag the Asset Criticality Rating slider to set the ACR.

9. (Optional) If you want to include a justification for your ACR change, in the Overwrite Reasoning section, select one or more reasons.

10. (Optional) If you want to include a note about your ACR change, in the Notes section, type a note.

11. Click Save.

    Tenable.io saves the custom ACR for all selected assets.
Lumin Data Timing

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

You must run scans to generate vulnerability data for use in Lumin views.

- **Time to Display Tenable.io Scan Result Data**
- **Time to Synchronize Data from Tenable.sc**
- **Time to Calculate or Recalculate Your CES, Assessment Maturity, or Remediation Maturity Grade**

**Time to Display Tenable.io Scan Result Data**

Vulnerability data generated by Tenable.io scans appears in Lumin views immediately upon scan completion.

Newly generated data does not immediately impact your Lumin metrics (for example, your CES). Tenable requires additional time to recalculate your metrics. For more information, see **Time to Calculate or Recalculate Your CES, Assessment Maturity, or Remediation Maturity Grade**.

**Time to Synchronize Data from Tenable.sc**

Vulnerability and asset data synchronize differently to Tenable.io.

<table>
<thead>
<tr>
<th>Data</th>
<th>Synchronization Method</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability data</td>
<td>• Manual initial synchronization.</td>
<td>After you initiate a synchronization, Tenable.sc immediately begins transferring data to Tenable.io. After 10-15 minutes, data begins appearing in Tenable.io. Newly transferred data does not immediately impact your Lumin metrics (for example, your CES). Tenable requires up to 48 hours to recalculate your metrics.</td>
</tr>
<tr>
<td></td>
<td>• Automatic subsequent synchronizations when new scan result data imports to your synchronized repositories.</td>
<td></td>
</tr>
</tbody>
</table>
# Data Synchronization Method Timing

<table>
<thead>
<tr>
<th>Data</th>
<th>Synchronization Method</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset data (tags in Tenable.io)</td>
<td>Manual (on-demand) synchronizations only.</td>
<td>All data and recalculated Lumin metrics appear in Tenable.io within 48 hours.</td>
</tr>
</tbody>
</table>

For more information about Tenable.sc synchronization, see [Lumin Synchronization](#) in the Tenable.sc User Guide.

## Time to Calculate or Recalculate Your CES, Assessment Maturity, or Remediation Maturity Grade

Tenable.io takes 24-48 hours to calculate or recalculate your metrics after any of the following events:

- You run your first Tenable.io-configured scans after licensing Lumin.
- You initiate your first Tenable.sc synchronization after licensing Lumin.
- Tenable.io runs a scan.
- Tenable.sc runs a scan that imports new data to a synchronized repository.

**Tip:** Tenable.io calculates Lumin metrics based on your licensed assets seen in the last 90 days. If you make changes to your scanning configuration (for example, you perform a recommended action to increase your Assessment Maturity grade), your changes influence the next scheduled recalculation, but take additional time over the next 90 days to significantly impact and overhaul your metrics.
View the Lumin Dashboard

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable Lumin

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

The Tenable-provided Lumin dashboard visualizes Cyber Exposure data for your organization. You cannot customize the widgets on this Tenable-provided dashboard.

To view summary data in the Lumin dashboard

1. Navigate to the new Tenable.io interface, as described in [Access the New Interface](#).
2. In the upper-left corner, click the button.
   
   The left navigation plane appears.
3. In the left navigation plane, click Lumin.
   
   The Lumin dashboard appears.

   **Note:** All Lumin data reflects all assets within the organization's Tenable.io instance.

4. Do any of the following:
   
   - Interact with the Lumin Dashboard Widgets.
   - Export the Lumin dashboard.
   - Update the Lumin industry benchmark.
Export the Lumin Dashboard Landing Page

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable Lumin

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

In Tenable.io, you can export the Lumin dashboard landing page.

To export the Lumin dashboard landing page:

1. **View** the Lumin dashboard.

2. In the upper-right corner, click **Export**.
   
   A drop-down menu appears.

3. From the drop-down menu, select one of the following options:
   
   - Click **PDF** to export the dashboard in PDF format.
   - Click **PNG** to export the dashboard in PNG format.
   - Click **JPG** to export the dashboard in JPG format.

   An **In Progress** message appears.

   Once the export completes, a **Success** message appears and Tenable.io downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.
Export a Widget from the Lumin Dashboard

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Required Additional License: Tenable Lumin

Required Tenable.io Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

In Tenable.io, you can export individual widgets from the Lumin dashboard.

Note: You cannot export the Cyber Exposure Score by Business Context widget.

To export a widget from the Lumin dashboard:

1. View the Lumin dashboard.
2. In the header of the widget you want to export, click the ••• button.
   
   A drop-down menu appears.
3. From the drop-down menu, select one of the following options:
   
   - Click PDF to export the dashboard in PDF format.
   - Click PNG to export the dashboard in PNG format.
   - Click JPG to export the dashboard in JPG format.
   
   An In Progress message appears.

   Once the export completes, a Success message appears and Tenable.io downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.
Update the Lumin Industry Benchmark

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable Lumin

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

Larger organizations may have business units that span multiple industries, or that don't fit neatly into one industry categorization. By selecting the most applicable industry benchmark in Lumin, users can maximize the relevancy of their data and more accurately track how their Lumin metrics compare with others across similar industries.

To update the Lumin industry benchmark:

1. Navigate to the new Tenable.io interface, as described in [Access the New Interface](#).

2. In the upper-left corner, click the menu button.

   The left navigation plane appears.

3. In the left navigation plane, click Lumin.

   The Lumin dashboard appears.

4. In the upper-right corner, click Configure.

   The Configure plane appears.

5. In the Benchmark section, from the Industry drop-down, select the industry benchmark you want to use across the Lumin dashboard.

6. Click Save.

   An Industry Updated confirmation message appears, and Tenable.io applies the new industry across the Lumin dashboard.

(Optional) To reset the Lumin industry benchmark:
1. On the **Configure Industry** plane, click **Reset to Default**.

   A confirmation message appears.

2. Click **Confirm**.

   An **Industry Updated** confirmation message appears, and Tenable.io resets the industry back to the industry selected upon account creation.
Exclude or Include Assets with Predicted Scores from your CES

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Required Additional License: Tenable Lumin

Required Tenable.io Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

By default, Lumin calculates your Cyber Exposure Score using predicted asset data. This means that when an asset does not have sufficient scan data, Lumin uses an algorithm to predict your CES. In some cases, you may want to exclude predicted data from your overall CES calculations to isolate the contribution of risk in your score. Selecting Exclude assets with predicted scores excludes assets with predicted data from both your current and historical CES calculations.

Note: This setting only impacts the CES and AES visible to your user account, but not the scores visible to other user accounts across your Tenable.io instance.

Tip: Tenable recommends including assets with predicted scores for the most comprehensive view of your Cyber Exposure.

To exclude or include assets with predicted scores from your CES:

1. Navigate to the new Tenable.io interface, as described in Access the New Interface.

2. In the upper-left corner, click the ☢ button.

   The left navigation plane appears.

3. In the left navigation plane, click Lumin.

   The Lumin dashboard appears.

4. In the upper-right corner, click Configure.

   The Configure plane appears. In the Cyber Exposure Score (CES) Calculations section, Lumin displays the number of known assets, predicted assets, and the total number of assets included in your CES.
5. Select or deselect the **Exclude assets with predicted scores** check box:

   - **Selected** – Lumin excludes assets with predicted scores from your CES calculation.
   - **Deselected** – Lumin includes assets with predicted scores from your CES calculation.

   At the bottom of the panel, a message summarizes how your CES will change.

6. Click **Save**.

   A confirmation message appears and Lumin automatically updates the Lumin dashboard data to include or exclude predicted assets from current and historical CES calculations.
Lumin Dashboard Widgets

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

The Lumin dashboard consists of the following widgets:

- Cyber Exposure Score
- Cyber Exposure Score Trend
- Actions to Reduce CES
- Assessment Maturity
- Remediation Maturity
- Cyber Exposure Alerts
- Mitigations
- Cyber Exposure Score by Business Context/Tag

**Note:** All Lumin data reflects all assets within the organization’s Tenable.io instance.

Cyber Exposure Score

*How does your overall risk compare to other Tenable customers in your Salesforce industry and the larger population?*

<table>
<thead>
<tr>
<th>Time Frame</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Past 90 days</td>
<td>Licensed assets for your entire organization</td>
</tr>
</tbody>
</table>

This widget summarizes the CES for your entire organization compared to Tenable customers in your Salesforce industry and the larger population.

**Note:** You can include or exclude assets with predicted scores from your CES. For more information, see [Exclude or Include Assets with Predicted Scores from your CES].

In this widget, you can perform the following actions:
• View a visual representation of your CES compared to the average CES for Tenable customers in your Salesforce industry and the larger population.

• View a summary statement about whether your CES recently increased or decreased.

• To view details about your CES, click your CES value.

  The Lumin Cyber Exposure Score details panel appears. For more information, see CES Details.

• Export the dashboard widget.

Cyber Exposure Score Trend

*How has the overall risk for your entire organization changed over time?*

<table>
<thead>
<tr>
<th>Time Frame</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Past 90 days at each point on the graph, recalculated daily</td>
<td>Licensed assets for your entire organization</td>
</tr>
</tbody>
</table>

This widget graphs the increases and decreases to your CES and to the average CES for Tenable customers in your Salesforce industry and the larger population.

In this widget, you can perform the following actions:

• To view details about an industry or population CES value on a specific date, hover over a point on the graph.

  The hover text provides historical data about the CES.

• To view details about your CES value on a specific date, click a point on the You line.

  The Lumin Cyber Exposure Score details plane appears. For more information, see CES Details.

• To show or hide data for your organization, the industry, or the population, click the boxes in the graph legend.

  The system updates the widget to show or hide the data you selected.

• Export the dashboard widget.
Actions to Reduce CES

What would the impact be if you addressed all of your top 20 recommended actions?

<table>
<thead>
<tr>
<th>Time Frame</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Past 90 days</td>
<td>Licensed assets for your entire organization</td>
</tr>
</tbody>
</table>

This widget summarizes the impact of your top 20 recommended actions.

In this widget, you can perform the following actions:

- View the expected CES reduction if you address all top 20 recommended actions.
- View the number of vulnerability instances you would eliminate if you addressed all top 20 recommended actions.
- View the number of assets affected by your top 20 recommended actions.
- To view details about your top 20 recommended actions, click See Top Recommended Actions.
- Export the dashboard widget.

Tip: A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

Assessment Maturity

How frequently and thoroughly are you scanning your assets?

<table>
<thead>
<tr>
<th>Time Frame</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Past 90 days</td>
<td>Licensed assets for your entire organization</td>
</tr>
</tbody>
</table>

This widget summarizes the Assessment Maturity grade for your entire organization compared to Tenable customers in your Salesforce industry and the larger population.

In this widget, you can perform the following actions:
- View your Assessment Maturity grade compared to the average Assessment Maturity grade for Tenable customers in your Salesforce industry and the larger population.

- View a summary statement about whether your Assessment Maturity grade recently increased or decreased.

- To view historical details about your Assessment Maturity grade, hover over a point on the graph.

  The hover text provides historical data about the Assessment Maturity grade.

- To view more details about your Assessment Maturity grade, click More Details.

  The Lumin Assessment Maturity page appears. For more information, see View Assessment Maturity Details.

- Export the dashboard widget.

Remediation Maturity

_How quickly and thoroughly are you remediating vulnerabilities on your assets?_

<table>
<thead>
<tr>
<th>Time Frame</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Past 90 days</td>
<td>Licensed assets for your entire organization</td>
</tr>
</tbody>
</table>

This widget summarizes the Remediation Maturity grade for your entire organization compared to Tenable customers in your Salesforce industry and the larger population.

In this widget, you can perform the following actions:

- View your Remediation Maturity grade compared to the average Remediation Maturity grade for Tenable customers in your Salesforce industry and the larger population.

- View a summary statement about whether your Remediation Maturity grade recently increased or decreased.

- To view historical details about your Remediation Maturity grade, hover over a point on the graph.

  The hover text provides historical data about the Remediation Maturity grade.
• To view more details about your Remediation Maturity grade, click More Details.

The Lumin Remediation Maturity page appears. For more information, see View Remediation Maturity Details.

• Export the dashboard widget.

Cyber Exposure Alerts

What Tenable Research cyber security alerts should you be aware of?

<table>
<thead>
<tr>
<th>Time Frame</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 most recent alerts</td>
<td>Licensed assets for your entire organization</td>
</tr>
</tbody>
</table>

This widget shows the 6 most recent cyber security alerts provided by the Tenable research team. Lumin provides further details about how many assets are potentially impacted and a link to the Tenable blog post for the alert, where you can view further information and any required responses.

In this widget, you can perform the following actions:

• View cyber exposure alerts with one of the following severities:
  
  ○ Information (Low) – The alert contains information that may be of interest, but does not require an immediate response.
  
  ○ Advisory (Medium) – The alert contains warning information and may require a response.
  
  ○ Response (Critical) – The alert requires an immediate response.

• To view the severity of the alert, a brief description, and the date on which the alert was published, roll over one of the alerts in the widget.

• To view the percentage of your assets affected by the alert (assets where one of the CVEs associated with the alert is present as a vulnerability on the asset), roll over one of the rows in the Assets Affected column.

If an alert has a CVE but no assets are affected, or you have not yet scanned your assets for the vulnerability, then the Assets Affected column displays a value of 0%. If no CVE is
currently assigned to the alert, then the **Assets Affected** column displays a value of **Pending**. Once the CVE is calculated for the alert, Lumin updates the column with the appropriate value.

- To view your **vulnerabilities by asset** automatically filtered by the CVE associated with the alert, click one of the percentages in the widget.
- To view the Tenable blog post about the exposure alert, click one of the alerts in the widget.
- To view the **Trending Threats** page for an alert, click one of the alerts in the widget.
- **Export** the dashboard widget.

## Mitigations

*How are endpoint protection agents distributed on your assets?*

<table>
<thead>
<tr>
<th>Time Frame</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Past 90 days</td>
<td><strong>Licensed assets</strong> for your entire organization</td>
</tr>
</tbody>
</table>

This widget summarizes the distribution of endpoint protection agents on your assets.

If you run an authenticated scan based on the **Basic Network Scan** template or **Advanced Network Scan** template or an agent scan based on the **Basic Agent Scan** or **Advanced Agent Scan** template, Tenable automatically enables the **plugins required to detect** mitigations present on your assets. Lumin defines mitigations as endpoint protection agents, which include antivirus software, Endpoint Protection Platforms (EPPs), or Endpoint Detection and Response (EDR) solutions.

In this widget, you can perform the following actions:

- To view a list of assets in a Mitigations category, click one of the percentages in the widget.

  The **Assets** page appears, filtered by licensed assets, the mitigations category you selected, and the past 90 days. For more information, see **View Assets**.

**Note**: When accessing the **Assets** page from the Mitigations widget, you may see an asset count notification at the top of the page. This notification indicates the number of assets you have permission to view based on the **access group** to which you belong.
To view details about the endpoint protection agents detected on your assets, click **More Details**.

The Lumin **Mitigations** page appears. For more information, see **View Mitigations Details in Lumin**.

- **Export** the dashboard widget.

## Cyber Exposure Score by Business Context/Tag

*How do assets with different tags (unique business context) compare?*

<table>
<thead>
<tr>
<th>Time Frame</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Past 90 days</td>
<td>All licensed assets to which the selected tags apply</td>
</tr>
</tbody>
</table>

This widget summarizes data about the **CES** calculated for your entire organization and for assets with specific business context **tags**.

In this widget, you can perform the following actions:

- View data for the assets with each tag.
  - **CES** – The average CES for assets with the tag. A value of **N/A** indicates Tenable is calculating your CES.
  - **CES Trend** – A visual representation of your CES change over the past 180 days. A value of **N/A** indicates Tenable is processing your CES data or that there are 0 assets with this tag.
  - **14 Day Trend** – A summary of how the CES increased (↑) or decreased (↓) in the past 14 days. A value of **N/A** indicates Tenable is processing your CES data or that there are 0 assets with this tag.
  - **Assessment Maturity** – The **Assessment Maturity** grade for assets with the tag. A value of **N/A** indicates there are 0 licensed assets with the tag.

To view details about your Assessment Maturity grade for assets with a specific tag, in the **Assessment Maturity** column, click the grade.
The Lumin **Assessment Maturity** page appears, filtered by the tag you selected.

- **Remediation Maturity** – The **Remediation Maturity** grade for assets with the tag.

To view details about your Remediation Maturity grade for assets with a specific tag, in the **Remediation Maturity** column, click the grade.

The Lumin **Remediation Maturity** page appears, filtered by the tag you selected. For more information, see View Remediation Maturity Details.

- **Licensed Assets** – The number of licensed assets with the tag.

- **# Assets with High AES** – The number of assets with the tag and a high AES.

- **Reduce Tag CES** – Your expected tag-level CES reduction if you resolve all of the solutions for assets with this specific tag. A value of N/A indicates your expected reduction is 5 or fewer. Typically, you cannot significantly reduce your CES if many assets were scanned without authentication or if your assets are healthy and your risk is already low.

To view the recommended actions for assets with a specific tag, in the **Reduce Tag CES** column, click **See Actions**.

The Lumin **Recommended Actions** page appears, filtered by licensed assets and the tag you selected.

- To view details about the assets with a specific tag, click a row of the table.

The Lumin **Business Context/Tag Asset Details** page appears. For more information, see View Business Context/Tag Asset Details.

- To modify the tags that appear in the widget:
  1. Click the button.
  2. Click the **Configure** button.

    The widget editor plane appears.
  3. Do one of the following:
To reorder the tags in the widget:
   a. Click and hold the ☑️ button next to the tag you want to move.
   b. Drag the tag to the new location.
   c. Release the mouse button to drop the tag in the new location.

To delete a tag from the widget, click the 🔴 button.

To add a tag to the widget, click the ⚡ Add Tag button and specify the tag you want to add.

This widget can display data for up to 25 tags.

4. Click Save.

Tenable.io refreshes the widget.

To sort the table, see Tenable.io Tables.
View the CES Details Panel

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable Lumin

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

Use this page to browse CES details for your organization, or for assets with a specific business context tag.

To view CES details:

1. Navigate to the new Tenable.io interface, as described in [Access the New Interface].
2. In the upper-left corner, click the button.
   
   The left navigation plane appears.
3. In the left navigation plane, click Lumin.
   
   The Lumin dashboard appears.
4. Do one of the following:

   - To view CES details for your entire organization:
     
     a. Do one of the following:

        - To view current CES details, in the **Cyber Exposure Score** widget, click the CES value.
        - To view historical CES details, in the **Cyber Exposure Score Trend** widget, click a past point on the graph.

   - To view CES details for assets with a specific business context tag:
     
     a. In the **Cyber Exposure Score by Business Context/Tag** widget, click the tag for which you want to view asset details.
The Lumin **Business Context/Tag Asset Details** page appears, filtered by the tag you selected.

b. In the **Cyber Exposure Score Trend** widget, click a CES value.

The Lumin **Cyber Exposure Score** details plane appears.

<table>
<thead>
<tr>
<th>Section</th>
<th>Time Frame</th>
<th>Assets</th>
<th>Action</th>
</tr>
</thead>
</table>
| Score                  | Past 90 days | Licensed assets             | • View the CES for your entire organization and the average CES for other Tenable customers in your Salesforce industry and the larger population.  
                           |            |                             | • View the amount by which the score for your entire organization increased (↑) or decreased (↓) in the past 14 days. |
| Change Factors         | Past 14 days | Licensed assets             | • View the major events that contributed to your score change. Factors are grouped by the type of change:  
                           |            |                             | ○ **CES Algorithm** — Any changes related to the CES Algorithm Update. |
For more information, see the Lumin FAQ.

Note: This section only appears if the algorithm update affected your CES score.

- **Asset Composition Change** — Asset license changes, assets depth changes, etc.
- **Vulnerability Composition Change** — Remediation of vulnerabilities, the discovery of new vulnerabilities, etc.
- **Asset Exposure and ACR Change** — Any changes to your AES or ACR

- To view specific details about what changed, under any change factor group, click More Details.

  Lumin displays the amount by which specific drivers increased (↑) or decreased (↓) in the past 14 days.
<table>
<thead>
<tr>
<th><strong>Assets (#)</strong></th>
<th>All time</th>
<th><strong>Licensed and unlicensed assets</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>(Visible only when viewing current CES details)</td>
<td></td>
<td>• View the total number of assets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For each ACR category, view the following information:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ The percentage of assets with critical, high, medium, and low ACR values.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Tip:</strong> The percentages do not total to 100% if any of your assets are unscored.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ The total number of assets with critical, high, medium, and low ACR values.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ If the number of assets with critical, high, medium, and low ACR values has increased or decreased in the past 14 days, the amount by which the percentage of assets and the total number of assets increased (↑) or decreased (↓) during that time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To view a list of assets in an ACR category, click a per-</td>
</tr>
</tbody>
</table>
The **Assets** page appears, filtered by licensed assets and the ACR category you selected. For more information, see [View Assets](#).

Vulnerabilities (#)

(Visible only when viewing current CES details)

<table>
<thead>
<tr>
<th>Vulnerabilities (#)</th>
<th>All time</th>
<th>Licensed and unlicensed assets</th>
</tr>
</thead>
</table>

- View the total number of vulnerabilities present on the assets.
- For each **VPR** category, view the following information:
  - The percentage of vulnerabilities with critical, high, medium, and low VPR values.
    - **Tip:** The percentages do not total to 100% if any of your assets are unscored.
  - The total number of vulnerabilities with critical, high, medium, and low VPR values.
  - If the number of vulnerabilities with critical, high, medium, and low VPR values increased or decreased in the past 14 days, the
amount by which the percentage of vulnerabilities and the total number of vulnerabilities has increased (↑) or decreased (↓) during that time.

- To view a list of vulnerabilities in a VPR category, click a percentage.

The **Vulnerabilities** page appears, filtered by licensed assets and the VPR category you selected. For more information, see [View Vulnerabilities by Plugin](#).
View Assessment Maturity Details

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable Lumin

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

Tenable calculates a dynamic Assessment Maturity grade that represents your overall scanning depth and frequency. For more information, see Assessment Maturity.

To view Assessment Maturity details for all assets:

1. Navigate to the new Tenable.io interface, as described in Access the New Interface.
2. In the upper-left corner, click the button.

   The left navigation plane appears.
3. In the left navigation plane, click Assessment Maturity.

   The Assessment Maturity page appears and, by default, shows details for your entire organization.
4. (Optional) To change the tag filter applied to the page, in the upper left corner, select a tag from the drop-down list.

   Lumin filters the page by the tag you selected.

**Note:** All Lumin data reflects all assets within the organization’s Tenable.io instance.

<table>
<thead>
<tr>
<th>Section or Widget</th>
<th>Time Frame</th>
<th>Assets</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Past 90 days</td>
<td><strong>Licensed assets</strong></td>
<td>This section summarizes your Assessment Maturity grade, compared to Tenable customers in your Salesforce industry and the larger population.</td>
</tr>
</tbody>
</table>
• View a visual representation of your Assessment Maturity compared to the average Assessment Maturity for Tenable customers in your Salesforce industry and the larger population.

• To view a list of your licensed assets impacting your Assessment Maturity, click <count> Licensed Assets.

The **Assets** page appears, filtered by licensed assets and the past 90 days. For more information, see [View Assets](#).

• To view a list of your unlicensed assets that do not impact your Assessment Maturity, click <count> Not Licensed.

The **Assets** page appears, filtered by unlicensed assets and the past 90 days. For more information, see [View Assets](#).

<p>| Maturity Score Trend | Past 90 days at each point on the graph, recalculated daily | Licensed assets | This widget graphs the increases and decreases to your Assessment Maturity grade and to the average Assessment Maturity grade for Tenable customers in your Salesforce |</p>
<table>
<thead>
<tr>
<th>Grade Changing Over Time?</th>
<th>Past 90 days</th>
<th>Industry and the larger population.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- To view details about an Assessment Maturity grade on a specific date, hover over a point on the graph. The hover text provides historical data about the Assessment Maturity grade. - To show or hide data for your organization, the industry, or the population, click the boxes in the graph legend. The system updates the widget to show or hide the data you selected.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recommended Actions</th>
<th>Past 90 days</th>
<th>Licensed assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>What general actions can you take to improve your scanning health?</td>
<td></td>
<td>This widget provides Tenable-recommended best practices to generally improve your scanning health. - Review your recommended best practices. - To take action, click the link next to the description.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Depth Grade</th>
<th>Past 90 days</th>
<th>Licensed assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are you scanning your assets thoroughly enough?</td>
<td></td>
<td>This widget summarizes the Assessment Maturity depth grade for your entire organization, compared to Tenable customers in your Salesforce industry and the larger population.</td>
</tr>
</tbody>
</table>
Tip: Tenable calculates your depth grade based on your:

- Scan policy coverage – How many plugins were enabled in your scan policies?
- Authentication coverage – How many of your scans successfully used authentication for full vulnerability detection?

Tip: You can configure authentication in credentialed scans or agent scans.

- View a visual representation of your depth grade compared to the average depth grade for Tenable customers in your Salesforce industry and the larger population.
- View a summary statement about whether your depth grade recently increased or decreased.

| Authentication Coverage | Past 90 days | Licensed assets | This widget graphs your percentage of assets scanned with authentication and without authentication, compared to Tenable customers in your Salesforce industry and the larger population. You can optimize your authentication coverage by ensuring you scan with successful authentication so that all... |
Plugins run on your assets.

- View a visual representation of your authentication coverage compared to the average depth grade for Tenable customers in your Salesforce industry and the larger population.

- To view details, hover over a scan type cluster on the graph.
  
The hover text provides data about the scan type.

- To show or hide data for your organization, the industry, or the population, click the boxes in the graph legend.
  
The system updates the widget to show or hide the data you selected.

### Scan Policy Coverage

<table>
<thead>
<tr>
<th>How often are you performing scans with full plugin coverage?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Past 90 days</strong></td>
</tr>
</tbody>
</table>

**Licensed assets**

This widget graphs your percentage of scan policies that have full plugin coverage when run with authentication, compared to Tenable customers in your Salesforce industry and the larger population.

For example, a scan using the [Basic Network Scan](#) template achieves full scan policy coverage.
- View a visual representation of your scan policy coverage compared to the average scan policy coverage for Tenable customers in your Salesforce industry and the larger population.
- To view details, hover over the graph.
  The hover text provides data about the percentage of scans with full plugin coverage.
- To show or hide data for your organization, the industry, or the population, click the boxes in the graph legend.
  The system updates the widget to show or hide the data you selected.

<table>
<thead>
<tr>
<th>Frequency Grade</th>
<th>Past 90 days</th>
<th>Licensed assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are you scanning your assets frequently enough?</td>
<td>This widget summarizes the <strong>Assessment Maturity</strong> frequency grade for your entire organization, compared to Tenable customers in your Salesforce industry and the larger population.</td>
<td><strong>Tip:</strong> Tenable calculates your frequency grade based on how often you scan assets on your network.</td>
</tr>
</tbody>
</table>
- View a visual representation of your frequency grade compared to the average frequency grade for Tenable customers in your Salesforce industry and the larger population.

- View a summary statement about whether your frequency grade recently increased or decreased.

<table>
<thead>
<tr>
<th><strong>Scan Cycle</strong></th>
<th><strong>Asset Scan Frequency</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>How much time passes between your scans?</strong></td>
<td><strong>How often are you scanning your assets?</strong></td>
</tr>
<tr>
<td><strong>Past 90 days</strong></td>
<td><strong>Past 90 days</strong></td>
</tr>
<tr>
<td><strong>Licensed assets</strong></td>
<td><strong>Licensed assets</strong></td>
</tr>
<tr>
<td>This widget summarizes your average scan frequency, in days, compared to Tenable customers in your Salesforce industry and the larger population. Your scan cycle is the average number of days between scans for your assets.</td>
<td>This widget graphs the percentage of your assets being scanned daily, weekly, monthly, and quarterly, compared to Tenable customers in your Salesforce industry and the larger population.</td>
</tr>
</tbody>
</table>

- To view details about a scan frequency for a specific date range, hover over a point on the graph.

The hover text provides data about the scan frequency.
• To show or hide data for your organization, the industry, or the population, click the boxes in the graph legend.

The system updates the widget to show or hide the data you selected.
View Remediation Maturity Details

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable Lumin

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

Tenable calculates a dynamic Remediation Maturity grade that represents your overall vulnerability remediation responsiveness and coverage. For more information, see Remediation Maturity.

To view Remediation Maturity details for all assets:

1. Navigate to the new Tenable.io interface, as described in [Access the New Interface](#).
2. In the upper-left corner, click the button.
   - The left navigation plane appears.
3. In the left navigation plane, click Remediation Maturity.
   - The Remediation Maturity page appears.
4. (Optional) To change the tag filter applied to the page, in the upper left corner, select a tag from the drop-down list.
   - Lumin filters the page by the tag you selected.

**Note:** All Lumin data reflects all assets within the organization's Tenable.io instance.

<table>
<thead>
<tr>
<th>Section or Widget</th>
<th>Time Frame</th>
<th>Assets</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Past 90 days</td>
<td>Licensed assets</td>
<td>This section summarizes your Remediation Maturity grade, compared to Tenable customers in your Salesforce industry and the larger population.</td>
</tr>
</tbody>
</table>
View a visual representation of your Remediation Maturity compared to the average Remediation Maturity for Tenable customers in your Salesforce industry and the larger population.

To view a list of your licensed assets impacting your Remediation Maturity grade, click `<count> Licensed Assets`.

The Assets page appears, filtered by licensed assets and the past 90 days. For more information, see View Assets.

To view a list of your unlicensed assets that do not impact your Remediation Maturity grade, click `<count> Not Licensed`.

The Assets page appears, filtered by unlicensed assets and the past 90 days. For more information, see View Assets.

| Maturity Score Trend | Licensed assets | This widget graphs the increases and decreases to your Remediation Maturity compared to the average Remediation Maturity for Tenable customers in your Salesforce industry and the larger population. |
How is your Remediation Maturity grade changing over time? | calculated daily | Remedi-ation Maturity grade and to the average Remediation Maturity grade for Tenable customers in your Salesforce industry and the larger population.

- To view details about a Remediation Maturity grade on a specific date, hover over a point on the graph.
- To show or hide data for your organization, the industry, or the population, click the boxes in the graph legend.

The system updates the widget to show or hide the data you selected.

| Recommended Actions | Past 90 days | Licensed assets | This widget provides Tenable-recommended best practices to generally improve your remediation health.

- Review your recommended best practices.
- To take action, click the link in the description.

| Remediation Responsiveness Grade | Past 90 days | Licensed assets | This widget summarizes the Remediation Maturity remediation responsiveness grade for your entire organization, compared to Tenable customers in
remediating vulnerabilities?

your Salesforce industry and the larger population.

**Tip:** Tenable calculates your remediation responsiveness grade based on your:

- Average remediation time since discovery — How long do you take to remediate a vulnerability after it is first discovered (the **First Seen** date)?
- Average remediation time since publication — How long do you take to remediate a vulnerability after a plugin is first made available (the **Plugin Publication** date)?

- View a visual representation of your remediation responsiveness grade compared to the average remediation responsiveness grade for Tenable customers in your Salesforce industry and the larger population.
- View a summary statement about whether your remediation responsiveness grade recently increased or decreased.

<table>
<thead>
<tr>
<th>Average Remediation Time Since Dis-</th>
<th>Past 90 days</th>
<th><strong>Licensed assets</strong></th>
<th>This widget graphs the average time, in days, you took to remedi-</th>
</tr>
</thead>
</table>

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
<table>
<thead>
<tr>
<th><strong>covery</strong></th>
<th><strong>VPR category</strong> after the vulnerability was first discovered, compared to Tenable customers in your Sales-force industry and the larger population.</th>
</tr>
</thead>
<tbody>
<tr>
<td>How long does it take you to remediate a vulnerability after it is first discovered (the <strong>First Seen</strong> date)?</td>
<td>• To view details about the average time for a specific VPR category, hover over a point on the graph.</td>
</tr>
<tr>
<td><strong>Average Remediation Time Since Publication</strong></td>
<td>• To show or hide data for your organization, the industry, or the population, click the boxes in the graph legend.</td>
</tr>
<tr>
<td>How long does it take you to remediate a vulnerability after a plugin is first made available (the <strong>Plugin Publication</strong> date)?</td>
<td>The system updates the widget to show or hide the data you selected.</td>
</tr>
<tr>
<td>Past 90 days</td>
<td>This widget graphs the average time, in days, you took to remediate vulnerabilities in each <strong>VPR category</strong> after a plugin was first made available, compared to Tenable customers in your Sales-force industry and the larger population.</td>
</tr>
<tr>
<td><strong>Licensed assets</strong></td>
<td>• To view details about the average time for a specific VPR category, hover over a point on the graph.</td>
</tr>
<tr>
<td>Remediation Coverage Grade</td>
<td>Past 90 days</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>How thoroughly are you remediating vulnerabilities?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Table Header</td>
<td>Time Period</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td><strong>Remediation Coverage</strong></td>
<td>Past 90 days</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Average Vulnerabilities Per Asset</strong></td>
<td>Past 90 days</td>
</tr>
<tr>
<td>How many vulnerabilities, on average, are present on an asset?</td>
<td><strong>category</strong> present on your assets, compared to Tenable customers in your Salesforce industry and the larger population.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td>• To view details about the count for a specific VPR category, hover over a point on the graph.</td>
</tr>
<tr>
<td></td>
<td>• To show or hide data for your organization, the industry, or the population, click the boxes in the graph legend.</td>
</tr>
<tr>
<td></td>
<td>The system updates the widget to show or hide the data you selected.</td>
</tr>
</tbody>
</table>
View Business Context/Tag Asset Details

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable Lumin

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can use this page to view details about assets with a specific business context tag.

**Before you begin:**

- Add tags to assets, as described in [Add a Tag to an Asset](#).

**To view business context tag asset details:**

1. Navigate to the new Tenable.io interface, as described in [Access the New Interface](#).

2. In the upper-left corner, click the button.

   The left navigation plane appears.

3. In the left navigation plane, click **Business Context**.

   The **Business Context/Tag Asset Details** page appears.

4. (Optional) To change the tag filter applied to the page, in the upper left corner, select a tag from the drop-down list.

   Lumin filters the page by the tag you selected.

**Note:** All Lumin data reflects all assets within the organization’s Tenable.io instance.

<table>
<thead>
<tr>
<th>Section or Widget</th>
<th>Time Frame</th>
<th>Assets</th>
<th>Action</th>
</tr>
</thead>
</table>
| Tag summary       | All time   | Licensed and unlicensed | • View the name of the tag.  
|                   |            |        | • View the **CES** calculated |

---

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable,Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
<table>
<thead>
<tr>
<th><strong>Cyber Exposure Score Trend</strong></th>
<th><strong>Past 90 days at each point on the graph, recalculated daily</strong></th>
<th><strong>Licensed assets with the tag applied</strong></th>
</tr>
</thead>
</table>

How has the overall risk for this business context changed over time?

This widget graphs the increases and decreases to your tag-specific CES compared to the average organization-wide CES for Tenable customers in your Salesforce industry and the larger population.

- To view details about an organization-wide industry or population CES value on a specific date, hover over a point on the graph.

  The hover text provides historical data about the CES.

- To view details about your tag-specific CES value on a specific date, click a point on the **You** line.

  The Lumin Cyber Exposure Score details plane appears. For more information, see CES Details.

- To show or hide data for your organization, the
industry, or the population, click the boxes in the graph legend.

The system updates the widget to show or hide the data you selected.

| Asset Distribution by Asset Exposure Score (AES) | Past 90 days | Licensed assets with the tag applied and shared with your user account via access groups | This widget summarizes the number of vulnerabilities in each AES category.

- To view the recommended solutions for an AES category, click one of the `<Category> AES Solutions` links.

The Solutions page appears, filtered by the tag, licensed assets, and the AES category you selected. For more information, see View Solutions.

- To view the recommended solutions for all assets, click the All Solutions link.

The Solutions page appears, filtered by the tag and licensed assets. For more information, see View Solutions.

| Asset Criticality | Past 90 days | Licensed and | This widget visualizes the per- |
### Rating Breakdown

How critical are my assets?

- View the total number of scanned assets on your network.
- View the percentage of assets in each category: **Critical, High, Medium, Low**, and **Unclassified**.
- To view a list of assets, click a category on the graph.

The Assets page appears, filtered by the tag, licensed assets seen in the past 90 days, and the ACR category you selected. For more information, see View Assets.

### Asset Scan Distribution

What percentage of your assets are scanned with different methods?

This widget summarizes your asset scan distribution during the past 90 days.

- **Authenticated Scans** are run by a non-Agent scanner with credentialed scanning configured. **Agent Scans** are run by Agent scanners. All other scans are **Unauthenticated Scans**.
- View the total number of...
assets scanned on your network in the past 90 days.

- View the percentage of assets where the system performed authenticated, unauthenticated, or agent scans in the past 90 days.

- View the percentage of assets the system has not scanned in the past 90 days.

- To filter the data displayed in the widget, roll over the widget and click the filter button. Click the desired filter.

  Tenable.io refreshes the widget.

- To view the assets list, click a scan category.

  The **Assets** page appears, filtered by the tag, licensed assets seen in the past 90 days, the scan type you selected, and the **ACR** category filter applied to the widget. For more information, see [View Assets](#).
<table>
<thead>
<tr>
<th><strong>Asset Scan Frequency</strong></th>
<th><strong>Past 90 days</strong></th>
<th><strong>Licensed and unlicensed assets</strong> with the tag applied</th>
<th><strong>This widget visualizes the percentage of assets scanned on your network during periods in the past 90 days, compared to others in your Salesforce industry and the population.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>How often are you scanning your assets?</td>
<td></td>
<td></td>
<td>• View the percentage of assets scanned on your network at <strong>Daily, Weekly, Monthly, or Quarterly</strong> intervals.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• To show or hide data for your organization, the industry, or the population, click the boxes in the graph legend. The system updates the widget to show or hide the data you selected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• To filter the data displayed in the widget, roll over the widget and click the button. Click the desired filter. Tenable.io refreshes the widget.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• To view the assets list, click a bar on the graph. The <strong>Assets</strong> page</td>
</tr>
</tbody>
</table>
appears, filtered by the tag, licensed assets, the time period you selected, and the **ACR** category filter applied to the widget. For more information, see [View Assets](#).
View Your Lumin External Risk Rating

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable Lumin

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

The **External Risk Rating** page allows you to view your organization's Lumin metrics alongside your external security posture via an integration with SecurityScorecard.

To view your external risk rating:

1. Navigate to the new Tenable.io interface, as described in [Access the New Interface](#).
2. In the upper-left corner, click the ** button.
   
   The left navigation plane appears.
3. In the left navigation plane, in the Lumin section, click **External Risk Rating**.
   
   The **External Risk Rating** page appears.

This page includes the following widgets:

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
</table>
| Internal Exposure Report for Your Organization | This widget summarizes the CES for your entire organization compared to Tenable customers in your Salesforce industry and the larger population. 

In this widget, you can perform the following actions:

- View a visual representation of your CES compared to the average CES for Tenable customers in your Salesforce industry and the larger population.
- View a summary statement about whether your CES recently increased or decreased. |
To view details about your CES, click your CES value. The Lumin **Cyber Exposure Score** details panel appears. For more information, see [CES Details](#).

To view the **Cyber Exposure Score Details** page, click **More Details**.

For more information about widgets, see [Lumin Dashboard Widgets](#).

<table>
<thead>
<tr>
<th>Assessment Maturity</th>
<th>This widget summarizes the <strong>Assessment Maturity</strong> grade for your entire organization compared to Tenable customers in your Salesforce industry and the larger population.</th>
</tr>
</thead>
</table>

In this widget, you can perform the following actions:

- View your Assessment Maturity grade compared to the average Assessment Maturity grade for Tenable customers in your Salesforce industry and the larger population.
- View a summary statement about whether your Assessment Maturity grade recently increased or decreased.
- To view historical details about your Assessment Maturity grade, hover over a point on the graph.

The hover text provides historical data about the Assessment Maturity grade.

- To view more details about your Assessment Maturity grade, click **More Details**.

The Lumin **Assessment Maturity** page appears. For more information, see [View Assessment Maturity Details](#).

For more information about widgets, see [Lumin Dashboard Widgets](#).
| Remediation Maturity | This widget summarizes the Remediation Maturity grade for your entire organization compared to Tenable customers in your Salesforce industry and the larger population.

In this widget, you can perform the following actions:

- View your Remediation Maturity grade compared to the average Remediation Maturity grade for Tenable customers in your Salesforce industry and the larger population.

- View a summary statement about whether your Remediation Maturity grade recently increased or decreased.

- To view historical details about your Remediation Maturity grade, hover over a point on the graph.

  The hover text provides historical data about the Remediation Maturity grade.

- To view more details about your Remediation Maturity grade, click More Details.

  The Lumin Remediation Maturity page appears. For more information, see View Remediation Maturity Details.

For more information about widgets, see Lumin Dashboard Widgets. |
|---|---|
| External Security Posture Report for Your Organization | This widget shows your external security posture via an integration with SecurityScorecard. The data in this widget updates daily.

In this widget, you can perform the following actions:

- To view your external security posture, click View My Grade.

  The widget updates to display your current security posture grade compared to the average grade for Tenable cus- |
<table>
<thead>
<tr>
<th></th>
<th>customers in your Salesforce industry and the larger population.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• View the 10 major security categories on which your score is based.</td>
</tr>
<tr>
<td></td>
<td>• To view the SecurityScorecard page for a security category, click the category.</td>
</tr>
<tr>
<td></td>
<td>The SecurityScorecard website opens in your browser.</td>
</tr>
</tbody>
</table>
View Mitigations Details in Lumin

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable Lumin

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

If you run an authenticated scan based on the Basic Network Scan template or Advanced Network Scan template or an agent scan based on the Basic Agent Scan or Advanced Agent Scan template, Tenable automatically enables the plugins required to detect mitigations present on your assets. Lumin defines mitigations as endpoint protection agents, which include antivirus software, Endpoint Protection Platforms (EPPs), or Endpoint Detection and Response (EDR) solutions.

Then, you can use Lumin Mitigations data to assess whether your assets are covered properly with the endpoint protection agent software.

Certain plugins must be enabled in your authenticated and agent scans to detect endpoint protection agents on your assets. For more information, see [Plugins for Mitigation Detection](#).

Before you begin:

- Confirm the required plugins are enabled in your scans.
- Run your scans before checking the Mitigations page.

To view a list of endpoint protection agents on your assets:

1. Navigate to the new Tenable.io interface, as described in [Access the New Interface](#).
2. In the upper-left corner, click the button.  
   
   The left navigation plane appears.
3. In the left navigation plane, click Lumin.  
   
   The Lumin dashboard appears.
4. In the **Mitigations** widget, click **See Details**.

The Lumin **Mitigations** page appears.

**Note:** All Lumin data reflects all assets within the organization's Tenable.io instance.

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Exports</strong> button</td>
<td>Download previously-generated export files.</td>
</tr>
<tr>
<td>Date range selector</td>
<td>Change the date range for the mitigations table. For more information, see <strong>Tenable.io Tables</strong>.</td>
</tr>
<tr>
<td><strong>Filters</strong> box</td>
<td>Filter the data displayed in the mitigations table.</td>
</tr>
<tr>
<td><strong>Search</strong> box</td>
<td>Search the mitigations table by product name. For more information, see <strong>Tenable.io Tables</strong>.</td>
</tr>
<tr>
<td><strong>Mitigations</strong> table</td>
<td>In this table, you can:</td>
</tr>
<tr>
<td></td>
<td>• View information about each endpoint protection agent.</td>
</tr>
<tr>
<td></td>
<td>○ <strong>Product Name</strong> – The name of the endpoint protection agent.</td>
</tr>
<tr>
<td></td>
<td>○ <strong>Vendor Name</strong> – The name of the vendor that maintains the end-</td>
</tr>
<tr>
<td></td>
<td>point protection agent.</td>
</tr>
<tr>
<td></td>
<td>○ <strong>All Assets</strong> – The total number of assets with the endpoint</td>
</tr>
<tr>
<td></td>
<td>protection agent present.</td>
</tr>
<tr>
<td></td>
<td>○ <strong>Critical Assets</strong> – The total number of <strong>Critical ACR</strong> assets</td>
</tr>
<tr>
<td></td>
<td>with the endpoint protection agent present.</td>
</tr>
<tr>
<td></td>
<td>○ <strong>High Assets</strong> – The total number of <strong>High</strong> ACR assets with the</td>
</tr>
<tr>
<td></td>
<td>endpoint protection agent present.</td>
</tr>
<tr>
<td></td>
<td>○ <strong>Version</strong> – The version of the endpoint protection agent.</td>
</tr>
<tr>
<td></td>
<td>○ <strong>Last Detected</strong> – The date that a scan last detected the endpoint</td>
</tr>
<tr>
<td></td>
<td>protection agent on an asset.</td>
</tr>
<tr>
<td></td>
<td>• Sort, increase or decrease the number of rows per page, or navigate to</td>
</tr>
</tbody>
</table>
another page of the table. For more information, see Tenable.io Tables.

- Export mitigations.

- To view a list of assets with a specific endpoint protection agent present, click the asset count in the appropriate column:
  - All Assets to view all assets regardless of the asset ACR
  - Critical Assets to view Critical ACR assets
  - High Assets to view High ACR assets

The Assets page appears, filtered by licensed assets, ACR severity, the mitigation product name, the mitigation vendor name, the mitigation version, and the past 90 days. For more information, see View Assets.
Plugins for Mitigation Detection

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

To detect mitigations, you must enable the following plugins in your scan.

**Tip:** These plugins are automatically enabled in the following Tenable-provided scan templates: Advanced Network Scan, Basic Network Scan, Advanced Agent Scan, Basic Agent Scan.

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>12107</td>
<td>McAfee Antivirus Detection and Status</td>
</tr>
<tr>
<td>16192</td>
<td>Trend Micro Antivirus Detection and Status</td>
</tr>
<tr>
<td>20283</td>
<td>Panda Antivirus Detection and Status</td>
</tr>
<tr>
<td>20284</td>
<td>Kaspersky Anti-Virus Detection and Status</td>
</tr>
<tr>
<td>21162</td>
<td>Spybot Search &amp; Destroy Detection</td>
</tr>
<tr>
<td>21608</td>
<td>NOD32 Antivirus Detection and Status</td>
</tr>
<tr>
<td>21725</td>
<td>Symantec Antivirus Software Detection and Status</td>
</tr>
<tr>
<td>21726</td>
<td>Webroot SpySweeper Enterprise Detection</td>
</tr>
<tr>
<td>24232</td>
<td>BitDefender Antivirus Detection and Status</td>
</tr>
<tr>
<td>52668</td>
<td>F-Secure Anti-Virus Detection and Status</td>
</tr>
<tr>
<td>54845</td>
<td>Sophos Anti-Virus for Mac OS X Detection</td>
</tr>
<tr>
<td>54846</td>
<td>Sophos Anti-Virus Detection and Status (Mac OS X)</td>
</tr>
<tr>
<td>56567</td>
<td>Mac OS X XProtect Detection</td>
</tr>
<tr>
<td>56568</td>
<td>Mac OS X XProtect Installed</td>
</tr>
<tr>
<td>58580</td>
<td>Trend Micro ServerProtect Detection and Status (credentialed check)</td>
</tr>
<tr>
<td>67119</td>
<td>McAfee ePolicy Orchestrator Installed (credentialed check)</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>68997</td>
<td>Check Point ZoneAlarm Detection and Status</td>
</tr>
<tr>
<td>74038</td>
<td>McAfee VirusScan Enterprise for Linux Detection and Status</td>
</tr>
<tr>
<td>84432</td>
<td>AVG Internet Security Detection</td>
</tr>
<tr>
<td>87777</td>
<td>Avast Antivirus Detection and Status</td>
</tr>
<tr>
<td>87923</td>
<td>McAfee Application Control / Change Control Installed</td>
</tr>
<tr>
<td>87955</td>
<td>McAfee Agent Detection</td>
</tr>
<tr>
<td>87989</td>
<td>McAfee Agent Detection (Linux/MacOS)</td>
</tr>
<tr>
<td>88598</td>
<td>Symantec Endpoint Protection Installed (Unix Credentialed Check)</td>
</tr>
<tr>
<td>95470</td>
<td>McAfee Host Intrusion Prevention Installed</td>
</tr>
<tr>
<td>100131</td>
<td>McAfee Security Scan Plus Detection</td>
</tr>
<tr>
<td>106757</td>
<td>CylancePROTECT Detection</td>
</tr>
<tr>
<td>106758</td>
<td>CylancePROTECT Detection (Mac OS X)</td>
</tr>
<tr>
<td>112279</td>
<td>Windows Defender Advanced Threat Protection Installed (Windows)</td>
</tr>
<tr>
<td>124366</td>
<td>McAfee Endpoint Security and Module Detection</td>
</tr>
<tr>
<td>131023</td>
<td>Windows Defender Installed</td>
</tr>
<tr>
<td>131725</td>
<td>Sophos Anti-Virus Installed (Windows)</td>
</tr>
<tr>
<td>133843</td>
<td>VMware Carbon Black Cloud Endpoint Standard Installed (Windows)</td>
</tr>
<tr>
<td>133962</td>
<td>Sophos Anti-Virus Installed (Linux)</td>
</tr>
<tr>
<td>134216</td>
<td>VMware Carbon Black Cloud Endpoint Standard Installed (macOS)</td>
</tr>
<tr>
<td>134871</td>
<td>Trend Micro Apex One Server Installed (Windows)</td>
</tr>
<tr>
<td>135408</td>
<td>Trend Micro Deep Security Agent Installed (Linux)</td>
</tr>
<tr>
<td>135409</td>
<td>Trend Micro Deep Security Agent Installed (Windows)</td>
</tr>
<tr>
<td>ID</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>136760</td>
<td>BitDefender Endpoint Security Tools Status (Windows)</td>
</tr>
<tr>
<td>136761</td>
<td>BitDefender Endpoint Security Tools Detection (Windows)</td>
</tr>
<tr>
<td>138209</td>
<td>Symantec Critical System Protection/Data Center Security Agent (Windows)</td>
</tr>
<tr>
<td>138853</td>
<td>F-Secure PSB Computer Protection (Windows)</td>
</tr>
<tr>
<td>139913</td>
<td>Check Point Endpoint Security SandBlast Agent Installed (Windows)</td>
</tr>
<tr>
<td>139918</td>
<td>ClamAV Installed (Linux)</td>
</tr>
<tr>
<td>140633</td>
<td>CrowdStrike Falcon Sensor Installed (Windows)</td>
</tr>
</tbody>
</table>
Export Mitigations

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Required Additional License: Tenable Lumin

Required Tenable.io Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can export a list of mitigations and affected assets, if needed, to share the data with others in your organization.

To export mitigations and affected assets:

1. View mitigation details for your organization.

2. In the mitigations table, select the check boxes next to the mitigation or mitigations that you want to include in the export file.
   
   The action bar appears at the bottom of the page.

3. In the action bar, click the [→ button.
   
   The Lumin mitigations Export plane appears.

4. In the Type section, click the type of export you want to perform.
   
   • CSV - Mitigations – A single .csv file that includes the mitigations you selected.
   
   • CSV - Mitigations & Assets Affected – Two .csv files that include the mitigations you selected and the assets affected where those mitigations are present.

   The export begins and Tenable.io downloads the export as a tar.gz package. For more information about the data in the export files, see Mitigations Export File Contents.

What to do next:

• To download previously exported mitigation data, see View and Download Exported Mitigations.
Mitigations Export File Contents

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

You can export mitigations from the Mitigations page. Your export files contain the following data.

<table>
<thead>
<tr>
<th>Export Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mitigations_summary.csv — the Mitigations file</td>
<td></td>
</tr>
<tr>
<td>product_name</td>
<td>The name of the endpoint protection agent.</td>
</tr>
<tr>
<td>vendor_name</td>
<td>The name of the vendor that maintains the endpoint protection agent.</td>
</tr>
<tr>
<td>all_assets</td>
<td>The total number of assets with the endpoint protection agent present.</td>
</tr>
<tr>
<td>critical_assets</td>
<td>The total number of Critical ACR assets with the endpoint protection agent present.</td>
</tr>
<tr>
<td>high_assets</td>
<td>The total number of High ACR assets with the endpoint protection agent present.</td>
</tr>
<tr>
<td>version</td>
<td>The version of the endpoint protection agent.</td>
</tr>
<tr>
<td>last_detected</td>
<td>The date that a scan last detected the endpoint protection agent on an asset.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>mitigations_detail.csv — the Affected Assets file</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>product_name</td>
<td>The name of the endpoint protection agent.</td>
</tr>
<tr>
<td>vendor_name</td>
<td>The name of the vendor that maintains the endpoint protection agent.</td>
</tr>
<tr>
<td>version</td>
<td>The version of the endpoint protection agent.</td>
</tr>
<tr>
<td>last_detected</td>
<td>The date that a scan last detected the endpoint protection agent on an asset.</td>
</tr>
<tr>
<td>asset_uuid</td>
<td>The asset's UUID.</td>
</tr>
<tr>
<td>hostname</td>
<td>The asset's hostname.</td>
</tr>
<tr>
<td>ipv4</td>
<td>The asset's IPv4 address.</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>operating_system</td>
<td>The asset's operating system.</td>
</tr>
<tr>
<td>acr_score</td>
<td>The asset's ACR.</td>
</tr>
<tr>
<td>acr_severity</td>
<td>The <strong>ACR category</strong> of the ACR calculated for the asset.</td>
</tr>
<tr>
<td>aes_score</td>
<td>The <strong>AES</strong> for the asset.</td>
</tr>
<tr>
<td>aes_severity</td>
<td>The <strong>AES category</strong> of the AES calculated for the asset.</td>
</tr>
</tbody>
</table>
View and Download Exported Mitigations

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable Lumin

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

After you export mitigation or affected assets files, you can view and download them. You cannot view or download export files generated by other users.

Before you begin:

- Export a mitigation or affected assets file.

To view and download mitigation and affected asset exports files:

1. View mitigation details for your organization.
2. In the upper-right corner of the page, click \[
\text{Export}\].

   The Lumin mitigations Export plane appears.

3. In the exports table, click the row for the export you want to download.

   Tenable.io downloads the export file as a `tar.gz` package. For information about the data in the export files, see Mitigations Export File Contents.
View Recommended Actions

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable Lumin

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

Tenable provides a list of top 20 recommended actions (solutions) for assets on your network, regardless of your access group permissions. You can identify solutions, then drill into the solution details to understand the steps to address the vulnerability on your network.

Addressing vulnerabilities on your network lowers your CES and AES metrics.

To view the top 20 recommended solutions for all assets on your network:

1. Navigate to the new Tenable.io interface, as described in [Access the New Interface].
2. In the upper-left corner, click the button.

   The left navigation plane appears.
3. In the left navigation plane, click Lumin.

   The Lumin dashboard appears.
4. In the **Reduce Cyber Exposure Score** widget, click **See Top Recommended Actions**.

   The Lumin **Recommended Actions** page appears. The table sorts your top solutions (up to 20) by VPR category (Critical to Low) and then by decreasing **Assets Affected**.
5. (Optional) To change the tag filter applied to the page, in the upper left corner, select a tag from the drop-down list.

   Lumin filters the page by the tag you selected.

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary bar</td>
<td>View summary statistics about the expected impact if you address all of the solutions in the <strong>Recommended Actions</strong> table.</td>
</tr>
</tbody>
</table>
- Expected **CES** reduction if you resolve all of the top solutions.

- Number of vulnerability instances eliminated by the top solutions.

**Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

- Number of assets affected by the top solutions.

**Recommended Actions table**

- View information about each solution.
  
  - **Solution** — A description for the solution.
  
  - **Licensed Assets** — The total number of assets affected by the vulnerabilities addressed by the solution.
  
  - **CVEs** — The total number of individual CVEs addressed by the solution.
  
  - **CVE Instances** — The number of CVE instances addressed by the solution.
  
  - **Exploit Code Maturity** — The key driver value for the highest **VPR** for the vulnerabilities addressed by the solution.
  
  - **VPR** — The highest **VPR** for the vulnerabilities addressed by the solution.
  
  - **CVSS** — The highest CVSSv2 score (or CVSSv3 score, when available) for the vulnerabilities addressed by the solution.

- To view details for a solution, click a solution row.

  The **Solution Details** page appears. For more information, see [View Solution Details](#).

- To export solution data, see [Export Recommended Actions](#).

- To download previously exported solution data, see [View and Download Exported Recommended Actions](#).
Export Recommended Actions

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable Lumin

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can export a list of recommended actions (solutions) and affected assets, if needed, to share the data with others in your organization.

To export recommended actions and affected assets:

1. Navigate to the new Tenable.io interface, as described in [Access the New Interface](#).

2. Navigate to one of the Lumin **Recommended Actions** pages, as described in [View Recommended Actions](#).

   The Lumin **Recommended Actions** page appears.

3. In the table, select the check boxes next to the recommended actions that you want to include in the export file.

   The action bar appears at the bottom of the page.

4. In the action bar, click the [→] button.

   The Lumin recommended actions **Export** plane appears.

5. In the **Type** section, click the type of export you want to perform.

   - **CSV - Selected Actions** – A single .csv file that includes the recommended actions you selected.

   - **CSV - Selected Actions & Assets Affected** – Two .csv files that include the recommended actions you selected and the assets affected by those actions.

   The export begins and Tenable.io downloads the export as a .tar.gz package. For information about the data in the export files, see [Recommended Actions Export File Contents](#).
What to do next:

- To download previously exported solution data, see View and Download Exported Recommended Actions.
Recommended Actions Export File Contents

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

You can export recommended actions (solutions) from two recommended action pages. The export contents from each page are unique to that page.

- Recommended Actions Export for a Group of Assets
- Recommended Actions Export for All Assets

Recommended Actions Export for a Group of Assets

If you export recommended actions and assets affected files from the Recommended Actions page for a group of assets, your export files contain the following data.

<table>
<thead>
<tr>
<th>Export Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail.csv – the Assets Affected file</td>
<td></td>
</tr>
<tr>
<td>solution_id</td>
<td>The solution's UUID.</td>
</tr>
<tr>
<td>solution_title</td>
<td>A description for the solution.</td>
</tr>
<tr>
<td>asset_uuid</td>
<td>The asset's UUID.</td>
</tr>
<tr>
<td>hostname</td>
<td>The asset's hostname.</td>
</tr>
<tr>
<td>ipv4</td>
<td>The asset's IPv4 address.</td>
</tr>
<tr>
<td>operating_system</td>
<td>The asset's operating system.</td>
</tr>
<tr>
<td>cve_count</td>
<td>The number of vulnerabilities on this asset addressed by the solution.</td>
</tr>
<tr>
<td>cve_instance_count</td>
<td>The total number of vulnerability instances on this asset addressed by the solution.</td>
</tr>
</tbody>
</table>

Tip: A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.
solution.csv — the **Selected Actions** file

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>solution_id</td>
<td>The solution's UUID.</td>
</tr>
<tr>
<td>solution_title</td>
<td>A description for the solution.</td>
</tr>
<tr>
<td>assets_affected</td>
<td>The total number of assets affected by the vulnerabilities addressed by the solution.</td>
</tr>
<tr>
<td>cve_count</td>
<td>The total number of vulnerabilities addressed by the solution.</td>
</tr>
<tr>
<td>vpr</td>
<td>The highest VPR for the vulnerabilities addressed by the solution.</td>
</tr>
<tr>
<td>cvss</td>
<td>The highest CVSSv2 score (or CVSSv3 score, when available) for the vulnerabilities addressed by the solution.</td>
</tr>
</tbody>
</table>

**Recommended Actions Export for All Assets**

If you export recommended actions and assets affected files from the **Recommended Actions** page for **all assets**, your export files contain the following data.

<table>
<thead>
<tr>
<th>Export Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail.csv</td>
<td></td>
</tr>
<tr>
<td>solution_id</td>
<td>The solution's UUID.</td>
</tr>
<tr>
<td>solution_title</td>
<td>A description for the solution.</td>
</tr>
<tr>
<td>asset_uuid</td>
<td>The asset's UUID.</td>
</tr>
<tr>
<td>hostname</td>
<td>The asset's hostname.</td>
</tr>
<tr>
<td>ipv4</td>
<td>The asset's IPv4 address.</td>
</tr>
<tr>
<td>operating_system</td>
<td>The asset's operating system.</td>
</tr>
<tr>
<td>acr_score</td>
<td>The asset's ACR.</td>
</tr>
<tr>
<td>acr_severity</td>
<td>The ACR category of the ACR calculated for the asset.</td>
</tr>
<tr>
<td>aes_score</td>
<td>The AES for the asset.</td>
</tr>
</tbody>
</table>

**detail.csv — the **Assets Affected** file**
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aes_severity</td>
<td>The <strong>AES category</strong> of the AES calculated for the asset.</td>
</tr>
<tr>
<td>vuln_count</td>
<td>The number of vulnerabilities on this asset addressed by the solution.</td>
</tr>
<tr>
<td>vuln_instance_count</td>
<td>The total number of vulnerability instances on this asset addressed by the solution.</td>
</tr>
</tbody>
</table>

**Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

### summary.csv – the **Selected Actions** file

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>solution</td>
<td>The solution's UUID.</td>
</tr>
<tr>
<td>summary</td>
<td>A description for the solution.</td>
</tr>
<tr>
<td>assets_affected</td>
<td>The total number of assets affected by the vulnerabilities addressed by the solution.</td>
</tr>
<tr>
<td>vulnerabilities</td>
<td>The total number of vulnerabilities addressed by the solution.</td>
</tr>
<tr>
<td>exploit_code_maturity</td>
<td>The <strong>key driver</strong> value for the highest <strong>VPR</strong> for the vulnerabilities addressed by the solution.</td>
</tr>
<tr>
<td>vpr</td>
<td>The highest <strong>VPR</strong> for the vulnerabilities addressed by the solution.</td>
</tr>
<tr>
<td>cvss</td>
<td>The highest CVSSv2 score (or CVSSv3 score, when available) for the vulnerabilities addressed by the solution.</td>
</tr>
</tbody>
</table>
View and Download Exported Recommended Actions

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Required Additional License: Tenable Lumin

Required Tenable.io Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

After you export recommended action or affected asset files, you can view and download them. You cannot view or download export files generated by other users.

Before you begin:

- Export a recommended action or affected assets file, as described in Export Recommended Actions.

To view and download recommended actions and affected assets export files:

1. Navigate to the new Tenable.io interface, as described in Access the New Interface.
2. In the upper-left corner, click the  button.
   
   The left navigation plane appears.
3. In the left navigation plane, click Lumin.
   
   The Lumin dashboard appears.
4. Navigate to one of the Recommended Actions pages, as described in View Recommended Actions.
   
   The Lumin Recommended Actions page appears.
5. Click Export.
   
   The Lumin recommended actions Export plane appears.
6. In the table, click the row for the export you want to download.
Tenable.io downloads the export file as a tar.gz package. For information about the data in the export files, see Recommended Actions Export File Contents.
The Assets page provides insight into your organization's assets and their vulnerabilities.

This page contains top-level widgets that provide a snapshot of the asset scanning status, as well as a table that lists assets scans have identified in your network. The top-level widgets include:

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset by Tags</td>
<td>This widget lists the top 5 tags applied to the highest number of assets. For more information, see <a href="#">Tags</a></td>
</tr>
<tr>
<td>Asset Coverage</td>
<td>This widget summarizes how thoroughly your scans assessed your environment during the past 90 days.</td>
</tr>
<tr>
<td></td>
<td>• Authenticated Scans – Authenticated assessment scans configured to find vulnerabilities on assets.</td>
</tr>
<tr>
<td></td>
<td>• Unauthenticated Scans – Unauthenticated assessment scans configured to find vulnerabilities on assets.</td>
</tr>
<tr>
<td></td>
<td>• Detected Only – Scans configured to discover assets.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <a href="#">Discovery Scans vs. Assessment Scans</a>.</td>
</tr>
<tr>
<td>Statistics</td>
<td>This widget summarizes any asset that is currently counted as licensed. In that it has been scanned in the last 90 days.</td>
</tr>
</tbody>
</table>

You can do the following from the Assets page:

- [View Asset View](#)
- [View Assets](#)
- [View Asset Details](#)
- [View Asset Activity](#)
- [Move Assets to a Network](#)
About Assets

Tenable.io includes the ability to track assets that belong to your organization. Assets are entities of value on a network that can be exploited. This includes laptops, desktops, servers, routers, mobile phones, virtual machines, software containers, and cloud instances. By providing comprehensive information about the assets that belong to your organization, Tenable.io helps to eliminate potential security risks, identify under-utilized resources, and support compliance efforts.

Tenable.io automatically creates or updates assets when a scan completes or scan results are imported. Tenable.io attempts to match incoming scan data to existing assets using a complex algorithm. This algorithm looks at attributes of the scanned hosts and employs a variety of heuristics to choose the best possible match. If Tenable.io cannot find a match, the system assumes this is the first time Tenable.io has encountered the asset and creates a new record for it. Otherwise, if Tenable.io finds a matching asset, the system updates any properties that have changed since the last time Tenable.io encountered the asset.

In addition to vulnerability information, Tenable.io also attempts to gather various other information about the asset, including:

- Interfaces (IP address and MAC address)
- DNS Names
- NetBIOS Name
- Operating System
- Installed Software
- UUIDS (Tenable, ePO, BIOS)
- Whether an agent is present
**View Assets**

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Access Group Permissions:** Can View

To view assets in the new interface:

1. In the upper-left corner, click the ⌁ button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Asset View** section, click **Assets**.

   The **Assets** page appears.

   **Note:** When accessing the **Assets** page from the certain Lumin dashboard widgets, you may see an asset count notification at the top of the page. This notification indicates the number of assets you have permission to view based on the access group to which you belong.

On this page, you can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action buttons</td>
<td>• <strong>Export</strong> asset data.</td>
</tr>
<tr>
<td></td>
<td>• Change the table date range.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <strong>Tenable.io Tables</strong>.</td>
</tr>
<tr>
<td><strong>Filters</strong> box</td>
<td><strong>Filter</strong> the assets table.</td>
</tr>
<tr>
<td><strong>Search</strong> box</td>
<td>Search the assets table.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <strong>Tenable.io Tables</strong>.</td>
</tr>
<tr>
<td><strong>Saved Searches</strong> box</td>
<td><strong>Create</strong> a saved search, <strong>edit</strong> an existing saved search, or <strong>apply</strong> an existing saved search.</td>
</tr>
<tr>
<td><strong>Assets</strong> table</td>
<td>• View information about the asset.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong> –</td>
</tr>
</tbody>
</table>
The asset identifier. Tenable.io assigns this identifier based on the presence of certain asset attributes in the following order:

1. Agent Name (if agent-scanned)
2. NetBIOS Name
3. FQDN
4. IPv6 address
5. IPv4 address

For example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the Asset Name.

- **AES** — (Requires Lumin license) The AES for the asset.
  
  - If the AES icon has a solid border and a colored background (green), then the AES score is calculated with known data. The known AES score is calculated using the known ACR and VPR for the asset.
  
  - If the AES icon has a dotted border and a white background (red), then the AES score is calculated using predicted data. The predicted AES score is calculated using a predicted VPR and/or ACR.

- **ACR** — (Requires Lumin license) The
The asset's ACR.

- **IP** – The asset's IP address.
- **OS** – The asset's operating system.
- **Mitigations** – (Requires Lumin license) Basic mitigation details for the asset.
- **Last Seen** – The time and date when the credentialed scan ran on the asset.
- **Source** – The scanner type that first scanned the asset.

- **View** asset details.
- (Requires Lumin license) **Edit** an ACR.
- **Export** asset data.
- **Add** or **remove** an asset tag.
- **Delete** an asset.

To sort, increase or decrease the number of rows per page, or navigate to another page of the table, see **Tenable.io Tables**.
View Asset View

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To view the **Asset View** page from the navigation plane:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.
2. In the left navigation plane, click **Asset View**.
   
   The **Asset View** page appears.

To view the **Asset View** page from a dashboard:

1. Click the button.
   
   The **Dashboards** plane appears with a list of configured dashboards.
2. Click **Asset View**.
   
   The **Asset View** page appears.
Asset View

The Asset View page provides a single view of all of the assets in your environment. This can help security teams understand their full attack surface. On the Asset View page, you can view the following types of assets:

- Managed assets that have been assessed for vulnerabilities
- Unmanaged assets that have been discovered, but not yet assessed for vulnerabilities

This Tenable-provided dashboard visualizes actionable insights for your Tenable.io assets. You can roll over individual items to reveal additional information or click on items to drill down into details behind the data.

Note: The assets displayed on the Asset View page are determined by the access group to which you belong. For more information, see Access Groups.

Note: The Asset View page does not include assets from Tenable.io Web Application Scanning or Tenable.io Container Security.

On the Asset View page, you can interact with the following widgets:

<table>
<thead>
<tr>
<th>Widget</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistics</td>
<td>This widget summarizes the actionable metrics for your inventory during the past 90 days.</td>
</tr>
<tr>
<td></td>
<td>To view a list of assets, click the assets count or one of the recent discovery metrics. For more information, see View Asset Details.</td>
</tr>
<tr>
<td>Asset Coverage</td>
<td>This widget summarizes how thoroughly your scans assessed your environment during the last 90 days.</td>
</tr>
<tr>
<td></td>
<td>• Authenticated Scans — Authenticated scans configured to find vulnerabilities on assets.</td>
</tr>
<tr>
<td></td>
<td>• Unauthenticated Scans — Unauthenticated scans configured to find vulnerabilities on assets.</td>
</tr>
<tr>
<td></td>
<td>• Detected Only — Scans configured to discover assets.</td>
</tr>
<tr>
<td>Most Common Operating Systems</td>
<td>This widget summarizes the most common operating systems running on your assets, organized by percentage of your assets running each operating system.</td>
</tr>
<tr>
<td>Assets by Tags</td>
<td>This widget lists the top 50 tags applied to the highest number of assets. For more information, see Tags.</td>
</tr>
<tr>
<td>Assets Running Web Servers</td>
<td>This widget lists assets found by Nessus Plugins running on web servers.</td>
</tr>
<tr>
<td>Assets Running Docker Hosts</td>
<td>This widget lists assets found by Nessus Plugins running on docker hosts.</td>
</tr>
</tbody>
</table>

For more information about how to Discover and Assess in Tenable.io, in the upper-right corner, click the Discover and Assess button.
Discover and Assess

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

The Discover and Assess page highlights the asset discovery options available in Tenable.io. On the Discovery page, user role permissions determine the access to certain widgets. For example, an administrator can access the Cloud Connectors widget, but a standard user cannot.

To view the Discover and Assess page:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, in the Asset View section, click Discovery.
   
   The Discover and Assess page appears.

3. Click any of the following widgets:

<table>
<thead>
<tr>
<th>Widget</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Discovery Method</td>
<td>To find assets on your network:</td>
</tr>
<tr>
<td></td>
<td>a. Click <strong>Start Scan</strong>.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Create a Scan</strong> page appears.</td>
</tr>
<tr>
<td></td>
<td>b. Create a scan. For more information, see <strong>Create a Scan</strong>.</td>
</tr>
<tr>
<td>Cloud Connectors</td>
<td>To get real-time visibility into your cloud assets:</td>
</tr>
<tr>
<td></td>
<td>a. Click <strong>Set Up Connectors</strong>.</td>
</tr>
<tr>
<td><strong>Connectors</strong></td>
<td><strong>Connect to ServiceNow</strong></td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>The Connectors page appears.</td>
<td>To discover assets with your CMDB:</td>
</tr>
<tr>
<td>b. Configure a connector. For more information, see Connectors.</td>
<td>a. Click Learn More.</td>
</tr>
<tr>
<td></td>
<td>b. Configure a two way sync between Tenable.io and ServiceNow. For more information, see the ServiceNow Integration Guide.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Tenable.io. For more information, see Link a Sensor.</td>
<td></td>
</tr>
</tbody>
</table>
View Asset Details

Required Tenable.io Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Access Group Permissions: Can View

To view details for a specific asset in the new interface:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, in the Asset View section, click Assets.
   
   The Assets page appears.

3. In the assets table, click the asset where you want to view details.
   
   The Asset Details page appears.
# Asset Details

On the **Asset Details** page, you can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Top section</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Asset Name</strong></td>
<td>The asset identifier. Tenable.io assigns this identifier based on the presence of certain asset attributes in the following order:</td>
</tr>
<tr>
<td></td>
<td>1. Agent Name (if agent-scanned)</td>
</tr>
<tr>
<td></td>
<td>2. NetBIOS Name</td>
</tr>
<tr>
<td></td>
<td>3. FQDN</td>
</tr>
<tr>
<td></td>
<td>4. IPv6 address</td>
</tr>
<tr>
<td></td>
<td>5. IPv4 address</td>
</tr>
<tr>
<td></td>
<td>For example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the Asset Name.</td>
</tr>
<tr>
<td><strong>Asset Information</strong></td>
<td>View summary asset information.</td>
</tr>
<tr>
<td></td>
<td>This information includes:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Operating System</strong> – The operating system that a scan identified as installed on the asset.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IPv4 Addresses</strong> – The IPv4 addresses that scans have associated with the asset.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IPv6 Addresses</strong> – The IPv6 addresses that scans have associated with the asset.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Network</strong> – The name of the network object associated with scanners that identified the asset. The default network name is <strong>Default</strong>. For more information about networks, see <a href="#">Networks</a>.</td>
</tr>
<tr>
<td><strong>Right section</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Asset Criticality Rating

- View the current **ACR** for the asset.
- To edit the ACR to more accurately reflect your network or the needs of your organization, click the pencil button.

The Lumin **Edit Asset Criticality Rating** plane appears. For more information, see **Edit an ACR Manually**.

### Tags

- View asset tags applied to the asset.
  - **Add** tags to the asset by clicking the pencil button next to **Tags**.
  - **Remove** tags from the asset.
  - **Search** assets by a specific tag.

### Scan Information

View summary scan information.

This information includes:

- **First Seen** — The time and date when a scan first identified the asset.
- **Last Seen** — The date and time of the scan that most recently identified the asset.
- **Last Auth Scan** — The time and date of the last credentialed scan run on the asset.
- **Source** — The source of the scan that identified the asset.

### ACR Key Drivers

View information about the [key drivers](#) Tenable used to calculate the ACR for this asset.

### Lower section

#### Activity

View asset activity.

#### Vulnerabilities

- Refine the data in the vulnerabilities table. For more information, see [Tenable.io Tables](#).
- View the total number of vulnerabilities on the asset, next to the...
| Search box. | • Click the vulnerability row to view **vulnerability details**.
| Export vulnerability data for the asset. | • **Add** or **remove** asset tags.
| **Delete** an asset. | • **Launch** a remediation scan for a vulnerability or vulnerabilities seen on the asset.
| **Solution** *(Requires Lumin license)* | • View the recommended solutions for the asset.
|  | • **CVE Count** – The number of vulnerabilities on this asset addressed by the solution.
|  | • **VPR** – The highest **VPR** of the vulnerabilities included in the solution.
|  | • **CVSS** – The highest CVSSv2 score (or CVSSv3 score, when available) of the vulnerabilities included in the solution.
|  | • To sort, increase or decrease the number of rows per page, or navigate to another page of the table, see **Tenable.io Tables**.
View Asset Activity

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

In the asset **Activity** tab, you can view asset history to help you troubleshoot issues. You can see when your asset was discovered, seen, updated, tagged, or deleted, as well as relevant metadata about the activity. You can also search the asset activity log.

To view asset activity in the new interface:

1. In the upper-left corner, click the **button.
   
   The left navigation plane appears.

2. In the left navigation plane, in the **Asset View** section, click **Assets**.
   
   The **Assets** page appears.

3. In the assets table, click the asset where you want to view details.
   
   The asset details page appears.

4. Click the **Activity** tab.
   
   The asset activity events table appears.

5. Do the following:

   a. (Optional) Search for specific events by **Event** value. For more information, see **Tenable.io Tables**.

   b. Click an event row to view more details.

   The **Activity** details plane appears and displays metadata for the event. Depending on the event, the metadata can include information such as:

   - the scan that generated the event
   - the event date
- properties that were changed on the asset
- the user who performed the action.

**Tip:** To view the scan that generated an **Asset Discovered**, **Asset Seen**, or **Asset Updated** event, click the link to the scan under **Seen by**.
Manage Asset Tags

**Note:** This section describes the new interface. For information about asset tags in the classic interface, see Manage Asset Tags in the Classic Interface.

Add your own business context to assets by tagging them with descriptive metadata in Tenable.io. You can manually apply a tag to create a static group of assets. An asset tag is primarily composed of a *Category:Value* pair. For example, if you want to group your assets by location, create a *Location* category with the value *Headquarters*. For more information about tags, see Tags.

You can manage asset tags in any user role.

To manage tags in the new interface, use the following procedures:

- Add a Tag to an Asset
- Search Assets by Tag
- Remove a Tag from an Asset

**Tip:** Applying or removing a tag generates an entry in the asset’s activity log. You can view the activity log in the Activity tab of the Asset Details page.

**Note:** Tenable.io applies dynamic tags to any assets, regardless of access group scoping. As a result, it may apply tags you create to assets outside of access groups to which you belong.
Add a Tag to an Asset

Required Tenable.io Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Access Group Permissions: Can View

This procedure describes how to tag assets from the Assets page in the new Tenable.io interface. You can also tag assets from the Vulnerabilities by Assets page.

To add a tag to a single asset:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, in the Asset View section, click Assets.

   The Assets page appears.

3. (Optional) Refine the assets listed in the table. For more information, see Tenable.io Tables.

4. Do one of the following:

<table>
<thead>
<tr>
<th>Location</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assets</strong> page</td>
<td>a. In the assets table, roll over the asset you want to tag.</td>
</tr>
<tr>
<td></td>
<td>The action buttons appear in the row.</td>
</tr>
<tr>
<td></td>
<td>b. In the row, click the button.</td>
</tr>
<tr>
<td><strong>Assets</strong> page</td>
<td>a. In the assets table, select the check box for the asset.</td>
</tr>
<tr>
<td></td>
<td>The action bar appears at the bottom of the page.</td>
</tr>
<tr>
<td></td>
<td>b. On the action bar, click the button.</td>
</tr>
<tr>
<td><strong>Asset Details</strong> page</td>
<td>a. In the assets table, click the row of the asset you want to add a tag.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Asset Details</strong> page appears.</td>
</tr>
</tbody>
</table>
b. Click the **Vulnerabilities** tab.  

    The **Vulnerabilities** tab appears.

c. In the upper-right corner, click the **Actions** button.  

    The actions menu appears.

d. In the actions menu, click ✉ **Add Tag**.

    The **Add Tag** plane appears.

5. Do any of the following:

   - Under **Recently Used Tags**, select a recently used tag.
   - Add a new or existing tag:
     a. In the **Category** box, type a category.  
        As you type, the list filters for matches.
     b. From the drop-down box, select an existing category, or if the category is new, click **Create "category name"**.
     c. In the **Value** box, type a value.  
        As you type, the list filters for matches.
     d. From the drop-down box, select an existing value, or if the value is new, click **Create "value"**.

    **Note:** The system does not save new tags you create by this method until you add the new tags to the asset.

    The tag appears in the **Tags to be Added** box.

    **Tip:** To remove a tag from **Tags to be Added**, roll over the tag and click the ✗ button.

6. Click **Add**.
The assets table appears. A confirmation message also appears. Tenable.io adds the tags specified in **Tags to be Added** to the asset.

**To add a tag to multiple assets:**

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Asset View** section, click **Assets**.

   The **Assets** page appears.

3. Select the assets where you want to add the tag:
   - To select assets individually, select the check box next to any asset.
   - To select all assets on the current page, select the check box in the asset table header row.

4. In the bottom action bar, click the button.

   The **Add Tag** plane appears.

5. Do any of the following:
   - Under **Recently Used Tags**, select a recently used tag.
   - Add a new or existing tag:
     - In the **Category** box, type a category.
       As you type, the list filters for matches.
     - From the drop-down box, select an existing category, or if the category is new, click **Create "category name"**.
     - In the **Value** box, type a value.
       As you type, the list filters for matches.
     - From the drop-down box, select an existing value, or if the value is new, click **Create "value"**.
**Note:** The system does not save new tags you create by this method until you add the new tags to the asset.

The tag appears in the **Tags to be Added** box.

**Tip:** To remove a tag from **Tags to be Added**, roll over the tag and click the $\times$ button.

6. Click **Add**.

The assets table appears. A confirmation message also appears. Tenable.io adds the tags specified in **Tags to be Added** to the assets.
Search Assets by Tag

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Access Group Permissions:** Can View

When you view an asset’s tags, you can search by a specific tag to create a filter for assets with the same tag. For more information on filters in the new interface, see [Filter a Table](#).

You can also search for assets by the tags table, as described in [Search for Assets by Tag from the Tags Table](#).

Before you begin:

- Add tags to assets, as described in [Add a Tag to an Asset](#).

To search assets by tag in the new interface:

1. View asset details.
2. In the left section, under Tags, roll over the tag you want to search by.
   
   The \( \downarrow \) button appears next to the tag.
3. Click the \( \downarrow \) button.
   
   A drop-down list appears.
4. In the drop-down list, click **Search Assets by Tag**.
   
   The Assets page appears. Tenable.io displays the Assets automatically filters the table for assets where the selected tag is applied.
Remove a Tag from an Asset

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Access Group Permissions:** Can View

This procedure describes how to remove tags from assets from the **Assets** page in the new interface. You can also remove asset tags from the **Vulnerabilities by Assets** page.

If an asset matches a dynamic tag's rules but you do not want the tag applied, you can manually remove a dynamic tag from the asset. If you later want to re-apply the dynamic tag to the asset where you removed the tag, you can remove the asset from the excluded assets list, as described in **Edit Tag Rules**.

To remove a tag from a single asset:

1. In the upper-left corner, click the **☰** button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Asset View** section, click **Assets**.

   The **Assets** page appears.

3. Do one of the following:

<table>
<thead>
<tr>
<th>Location</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assets</strong></td>
<td>a. In the assets table, roll over the asset where you want to remove a tag.</td>
</tr>
<tr>
<td></td>
<td>The action buttons appear in the row.</td>
</tr>
<tr>
<td></td>
<td>b. In the row, click the <strong>🗑️</strong> button.</td>
</tr>
<tr>
<td></td>
<td>c. Click the ** gridSize ** button.</td>
</tr>
<tr>
<td><strong>Assets</strong></td>
<td>a. In the assets table, select the check box for each asset from which you want to remove a tag.</td>
</tr>
</tbody>
</table>
The action bar appears at the bottom of the page.

b. On the action bar, click the button.

| Asset Details page | a. In the assets table, click the asset where you want to remove the tag.  
| | The Asset Details page appears.  
| | b. Click the Vulnerabilities tab.  
| | The Vulnerabilities tab appears.  
| | c. In the upper-right corner, click the Actions button.  
| | The actions menu appears.  
| | d. In the actions menu, click Remove Tag.  

The Remove Tags plane appears.

4. Under Current Tags, click each tag you want to remove.

The tag appears in the Tags to be Removed box.

**Tip:** To remove a tag from Tags to be Removed, roll over the tag and click the button.

5. Click Remove.

Tenable.io removes the tags specified in Tags to be Removed from the asset.

To remove tags from multiple assets:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, in the Asset View section, click Assets.

   The Assets page appears.

3. In the assets table, click the check box next to each asset for which you want to remove the tag.
The action bar appears at the bottom of the page.

4. In the action bar, click the button.

The Remove Tags plane appears.

5. Under Current Tags, click each tag you want to remove.

The tag appears in the Tags to be Removed box.

**Tip:** To remove a tag from Tags to be Removed, roll over the tag and click the button.

6. Click Remove.

Tenable.io removes the tags specified in Tags to be Removed from the selected assets.

Tip: To remove a tag from Tags to be Removed, roll over the tag and click the button.
Export Asset Data

Required Tenable.io Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Access Group Permissions: Can View

To export asset data in the new interface:

1. In the upper-left corner, click the button.
   The left navigation plane appears.

2. In the left navigation plane, in the Asset View section, click Assets.
   The Assets page appears.

3. (Optional) Refine the table data. For more information, see Tenable.io Tables.

4. (Optional) Apply a saved search to the table.

5. Select the assets you want to export:

<table>
<thead>
<tr>
<th>Export Scope</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>All assets</td>
<td>To export all assets, in the upper-right corner of the page, click the Export button.</td>
</tr>
<tr>
<td>Selected assets</td>
<td>To export selected assets:</td>
</tr>
<tr>
<td></td>
<td>a. In the assets table, select the check box for each asset you want to export.</td>
</tr>
<tr>
<td></td>
<td>The action bar appears at the bottom of the page.</td>
</tr>
<tr>
<td></td>
<td>b. In the action bar, click the button.</td>
</tr>
<tr>
<td>A single asset</td>
<td>To export a single asset:</td>
</tr>
<tr>
<td></td>
<td>a. In the assets table, roll over the asset you want to export.</td>
</tr>
</tbody>
</table>
The action buttons appear in the row.

b. Click the [→] button.

The **Exports** plane appears. This plane contains:

- A brief description of the export scope you selected under the **Export** label. This description specifies the number of assets you selected for the export.

- A list of available export formats.

6. Click the export format you want to use:

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSV</td>
<td>.csv text file.</td>
</tr>
</tbody>
</table>

A list of export fields appears. You can select which fields the export includes by selecting the check box next to any field. To view only the selected fields, click **View Selected**.

For more information, see [CSV Asset Export Fields](#).

**Note:** When you export assets for the first time, all fields are selected. If you modify the field selection, Tenable.io retains your selections as the default the next time you generate an export file.

Tenable.io begins processing the export. Depending on the size of the exported data, Tenable.io may take several minutes to process the export.

When processing completes, Tenable.io downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

7. Access the export file via your browser’s downloads directory.
## CSV Asset Export Fields

Each line in the .csv file is composed of the fields described in the following table. On the Assets page, you can export assets as a .csv file.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACR Drivers</td>
<td>(Requires Lumin license) The key drivers Tenable used to calculate the ACR for this asset.</td>
</tr>
<tr>
<td>ACR Score</td>
<td>(Requires Lumin license) The asset's ACR.</td>
</tr>
<tr>
<td>Agent Name</td>
<td>The name of the Nessus agent that scanned and identified the asset.</td>
</tr>
<tr>
<td>AWS Availability Zone</td>
<td>The name of the Availability Zone where AWS hosts the virtual machine instance. For more information, see Regions and Availability Zones in the AWS documentation.</td>
</tr>
<tr>
<td>AWS EC2 Instance AMI ID</td>
<td>The unique identifier of the Linux AMI image in Amazon Elastic Compute Cloud (Amazon EC2). For more information, see the Amazon Elastic Compute Cloud Documentation.</td>
</tr>
<tr>
<td>AWS EC2 Instance Group Name</td>
<td>The virtual machine instance's group in AWS.</td>
</tr>
<tr>
<td>AWS EC2 Instance ID</td>
<td>The unique identifier of the Linux instance in Amazon EC2. For more information, see the Amazon Elastic Compute Cloud Documentation.</td>
</tr>
<tr>
<td>AWS EC2 Instance State Name</td>
<td>The state of the virtual machine instance in AWS at the time of the scan. For possible values, see API Instance State in the Amazon Elastic Compute Cloud Documentation.</td>
</tr>
<tr>
<td>AWS EC2 Instance Type</td>
<td>The type of virtual machine instance in Amazon EC2. Amazon EC2 instance types dictate the specifications of the instance (for example, how much RAM it has). For a list of possible values, see Amazon EC2 Instance Types in the AWS documentation.</td>
</tr>
<tr>
<td>AWS EC2 Name</td>
<td>The name of the virtual machine instance in Amazon EC2.</td>
</tr>
<tr>
<td>AWS EC2 Product</td>
<td>The product code associated with the AMI used to launch the virtual</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Code</td>
<td>machine instance in Amazon EC2.</td>
</tr>
<tr>
<td>AWS Owner ID</td>
<td>A UUID for the Amazon AWS account that created the virtual machine instance. For more information, see AWS Account Identifiers in the AWS documentation. This attribute contains a value for Amazon EC2 instances only. For other asset types, this attribute is empty.</td>
</tr>
<tr>
<td>AWS Region</td>
<td>The region where AWS hosts the virtual machine instance, for example, us-east-1. For more information, see Regions and Availability Zones in the AWS documentation.</td>
</tr>
<tr>
<td>AWS Subnet ID</td>
<td>The unique identifier of the AWS subnet where the virtual machine instance was running at the time of the scan.</td>
</tr>
<tr>
<td>AWS VPC ID</td>
<td>The unique identifier of the public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private Cloud User Guide.</td>
</tr>
<tr>
<td>Azure VM ID</td>
<td>The unique identifier of the Microsoft Azure virtual machine instance. For more information, see Accessing and Using Azure VM Unique ID in the Microsoft Azure documentation.</td>
</tr>
<tr>
<td>BigFix Asset ID</td>
<td>The unique identifiers of the asset in IBM BigFix. For more information, see the IBM BigFix documentation.</td>
</tr>
<tr>
<td>BIOS UUID</td>
<td>The BIOS UUID of the asset.</td>
</tr>
<tr>
<td>Created At</td>
<td>The time and date when Tenable.io created the asset record.</td>
</tr>
<tr>
<td>Deleted At</td>
<td>The time and date when a user deleted the asset record. When a user deletes an asset record, Tenable.io retains the record until the asset ages out of the license count.</td>
</tr>
<tr>
<td>Deleted By</td>
<td>The user who deleted the asset record.</td>
</tr>
<tr>
<td>Exposure Score</td>
<td>The [Asset Exposure Score (AES)] calculated for the asset.</td>
</tr>
<tr>
<td>First Scan Time</td>
<td>The time and date of the first scan run against the asset.</td>
</tr>
<tr>
<td><strong>First Seen</strong></td>
<td>The time and date when a scan first identified the asset.</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td><strong>FQDN</strong></td>
<td>The fully-qualified domain name of the host that the vulnerability was detected on.</td>
</tr>
<tr>
<td><strong>GCP Instance ID</strong></td>
<td>The unique identifier of the virtual machine instance in Google Cloud Platform (GCP).</td>
</tr>
<tr>
<td><strong>GCP Project ID</strong></td>
<td>The customized name of the project to which the virtual machine instance belongs in GCP. For more information, see Creating and Managing Projects in the GCP documentation.</td>
</tr>
<tr>
<td><strong>GCP Zone</strong></td>
<td>The zone where the virtual machine instance runs in GCP. For more information, see Regions and Zones in the GCP documentation.</td>
</tr>
<tr>
<td><strong>Has Agent</strong></td>
<td>Specifies whether a Nessus agent scan identified the asset.</td>
</tr>
<tr>
<td><strong>Has Plugin Results</strong></td>
<td>Specifies whether the asset has plugin results associated with it.</td>
</tr>
<tr>
<td><strong>Hostname</strong></td>
<td>The hostname of the asset.</td>
</tr>
<tr>
<td><strong>id</strong></td>
<td>The UUID of the asset in Tenable.io.</td>
</tr>
<tr>
<td><strong>Installed Software</strong></td>
<td>A list of Common Platform Enumeration (CPE) values that represent software applications a scan identified as present on an asset. This field supports the CPE 2.2 format. For more information, see the Component Syntax section of the CPE Specification documentation, Version 2.2. For assets identified in Tenable scans, this field contains data only if a scan using Nessus Plugin ID 45590 has evaluated the asset.</td>
</tr>
<tr>
<td><strong>Interfaces</strong></td>
<td>The network interfaces that scans identified on the asset.</td>
</tr>
<tr>
<td><strong>IPv4</strong></td>
<td>An IPv4 address for the asset.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IPv6</td>
<td>An IPv6 address for the asset.</td>
</tr>
<tr>
<td>Last Authenticated</td>
<td>The time and date of the last credentialed scan run on the asset.</td>
</tr>
<tr>
<td>Last Licensed Scan Date</td>
<td>The time and date of the last scan that identified the asset as licensed. For more information about licensed assets, see <a href="#">Vulnerability Management Licenses</a>.</td>
</tr>
<tr>
<td>Last Scan Target</td>
<td>The FQDN, IPv4 address, or IPv6 address that the scanner last used to target the asset.</td>
</tr>
<tr>
<td>Last Scan Time</td>
<td>The time and date of the last scan run against the asset.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>The date and time of the scan that most recently identified the asset.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>A MAC address that a scan has associated with the asset record.</td>
</tr>
<tr>
<td>Manufacturer TPM ID</td>
<td>The manufacturer's unique identifiers of the Trusted Platform Module (TPM) associated with the asset.</td>
</tr>
<tr>
<td>McAfee Epo Agent Guid</td>
<td>The unique identifier of the McAfee ePO agent that identified the asset. For more information, see the McAfee documentation.</td>
</tr>
<tr>
<td>McAfee EpoGuid</td>
<td>The unique identifier of the asset in McAfee ePolicy Orchestrator (ePO). For more information, see the McAfee documentation.</td>
</tr>
<tr>
<td>Mitigations</td>
<td>(Requires Lumin license) The mitigations that scans have identified as present on the asset. Lumin defines mitigations as endpoint protection agents, which include antivirus software, Endpoint Protection Platforms (EPPs), or Endpoint Detection and Response (EDR) solutions</td>
</tr>
<tr>
<td>NetBIOS Name</td>
<td>The NetBIOS name for the asset.</td>
</tr>
<tr>
<td>Network Id</td>
<td>The ID of the network object associated with scanners that identified the asset. The default network ID is 00000000-0000-0000-0000-000000000000. For more information about networks, see <a href="#">Networks</a>.</td>
</tr>
<tr>
<td>Operating System</td>
<td>The operating system that a scan identified as installed on the asset.</td>
</tr>
<tr>
<td>Qualys Asset ID</td>
<td>The Asset ID of the asset in Qualys. For more information, see the Qualys documentation</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>This field contains a value only for assets associated with Qualys vulnerabilities you import via the Tenable.io API. For more information, see the Tenable Developer Portal.</td>
<td></td>
</tr>
<tr>
<td>Qualys Host ID</td>
<td>The Host ID of the asset in Qualys. For more information, see the Qualys documentation. This field contains a value only for assets associated with Qualys vulnerabilities you import via the Tenable.io API. For more information, see Tenable Developer Portal.</td>
</tr>
<tr>
<td>Scan Frequency</td>
<td>The number of times the asset was scanned within the past 90 days.</td>
</tr>
<tr>
<td>ServiceNow Sys ID</td>
<td>The unique record identifier of the asset in ServiceNow. For more information, see the ServiceNow documentation.</td>
</tr>
<tr>
<td>Sources</td>
<td>The source of the scan that identified the asset. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>- Agent (Nessus Agent)</td>
</tr>
<tr>
<td></td>
<td>- Nessus (Nessus scan)</td>
</tr>
<tr>
<td></td>
<td>- PVS/NNM (Nessus Network Monitor)</td>
</tr>
<tr>
<td></td>
<td>- WAS (Web Application Scanning)</td>
</tr>
<tr>
<td></td>
<td>- AWS Connector</td>
</tr>
<tr>
<td></td>
<td>- Azure Connector</td>
</tr>
<tr>
<td></td>
<td>- GCP Connector</td>
</tr>
<tr>
<td></td>
<td>- Qualys Connector</td>
</tr>
<tr>
<td>SSH Fingerprint</td>
<td>The SSH key fingerprints that scans have associated with the asset record.</td>
</tr>
<tr>
<td>Symantec EP Hardware Key</td>
<td>The hardware keys for the asset in Symantec Endpoint Protection.</td>
</tr>
<tr>
<td>System Type</td>
<td>The system types as reported by Plugin ID 54615. For more information, see Tenable Plugins.</td>
</tr>
<tr>
<td><strong>Tags</strong></td>
<td>Category tags assigned to the asset in Tenable.io. For more information, see <a href="#">Tags</a>.</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Tenable UUID</strong></td>
<td>The UUID of the agent present on the asset. This attribute is empty if no agent is present on the asset.</td>
</tr>
<tr>
<td><strong>Terminated At</strong></td>
<td>The time and date when a user terminated the virtual machine instance of the asset (for example, in AWS).</td>
</tr>
<tr>
<td><strong>Terminated By</strong></td>
<td>The user who terminated the virtual machine instance of the asset.</td>
</tr>
<tr>
<td><strong>Updated At</strong></td>
<td>The time and date when the asset record was last updated.</td>
</tr>
</tbody>
</table>
Export Vulnerability Data for an Asset

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Access Group Permissions:** Can View

To export vulnerability data for an asset in the new interface:

1. **View** the asset details.
2. In the **Asset Details** page, click the **Vulnerabilities** tab.
3. (Optional) Refine the vulnerabilities table data. For more information, see [Tenable.io Tables](#).
4. Do one of the following:
   - **Select an individual vulnerability to export.**
     a. In the vulnerabilities table, roll over the vulnerability you want to export.
        
        The action button appears in the row.
     b. Click the [→ button.
        
        The **Export** plane appears.
   - **Select multiple vulnerabilities to export.**
     a. In the vulnerabilities table, click the check box next to any vulnerability you want to export.
        
        The action bar appears at the bottom of the page.
     b. In the action bar, click the [→ button.
        
        The **Export** plane appears.
5. In the **Export** plane, click the export format you want to use:
### Format and Description

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDF - Current</td>
<td>Adobe PDF file.</td>
</tr>
<tr>
<td>PDF - Executive Summary</td>
<td></td>
</tr>
<tr>
<td>HTML - Current</td>
<td>Web-based HTML file.</td>
</tr>
<tr>
<td>HTML - Executive Summary</td>
<td></td>
</tr>
<tr>
<td>Nessus</td>
<td>Nessus file. Nessus exports are the only file format that you can import into Tenable.io.</td>
</tr>
<tr>
<td>CSV</td>
<td>Comma Separated Values text file.</td>
</tr>
</tbody>
</table>

**Note:** Tenable.io supports [tag filters](#) in the CSV export format only.

6. Click **Export**.

Tenable.io begins processing the report. Depending on the size of the exported data, Tenable.io may take several minutes to process the report.

When processing completes, Tenable.io downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.
Delete Assets

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Required Access Group Permissions:** Can View

You can delete assets from the Assets page, the Asset Detail page, or the Vulnerability by Asset page.

When you delete an asset, Tenable.io deletes the asset from the default view of the assets table, deletes vulnerability data associated with the asset, and stops matching scan results to the asset.

Deleting an asset does not immediately subtract the asset from your licensed assets count. Deleted assets continue to be included in the count until they automatically age out of your licensed assets count after 90 days.

To delete a single asset:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. Do one of the following:

<table>
<thead>
<tr>
<th>Location</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assets</strong> page</td>
<td>a. View the assets table.</td>
</tr>
<tr>
<td></td>
<td>b. In the assets table, roll over the asset you want you want to delete.</td>
</tr>
<tr>
<td></td>
<td>The action buttons appear in the row.</td>
</tr>
<tr>
<td></td>
<td>c. In the row, click the button.</td>
</tr>
<tr>
<td></td>
<td>A menu appears.</td>
</tr>
<tr>
<td></td>
<td>d. Click Delete.</td>
</tr>
<tr>
<td></td>
<td>A confirmation window appears.</td>
</tr>
<tr>
<td>Assets Details page</td>
<td>a. View the asset details.</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td></td>
<td>b. In the upper-right corner, click the Actions button.</td>
</tr>
<tr>
<td></td>
<td>The actions menu appears.</td>
</tr>
<tr>
<td></td>
<td>c. In the actions menu, click Delete.</td>
</tr>
<tr>
<td></td>
<td>A confirmation window appears.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vulnerabilities by Assets</th>
<th>a. View vulnerabilities by asset.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>b. In the assets table, roll over the asset you want to delete.</td>
</tr>
<tr>
<td></td>
<td>The action buttons appear in the row.</td>
</tr>
<tr>
<td></td>
<td>c. In the row, click the button.</td>
</tr>
<tr>
<td></td>
<td>A confirmation window appears.</td>
</tr>
</tbody>
</table>

3. In the confirmation window, click Delete.

Tenable.io deletes the asset.

To delete multiple assets:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. Do one of the following:
   - View your assets.
   - View your vulnerabilities by asset.

3. In the assets table, click the check box next to each asset you want to delete.

   The action bar appears at the bottom of the page.

4. In the action bar, click the button.

   A confirmation window appears.

5. In the confirmation window, click Delete.
Tenable.io deletes the selected assets.

To delete all assets:

1. [View](#) your assets.
2. In the asset table header row, select the check box to select all assets on the current page.
   
   The action bar appears at the bottom of the page.
3. In the action bar, click *(Select All Assets)* to select all remaining assets.
4. In the action bar, click the ![button](image) button.
   
   A confirmation window appears.
5. In the confirmation window, click **Delete**.

   Tenable.io deletes all assets.
View Deleted Assets

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Access Group Permissions:** Can View

You can view information about deleted assets until they age out of your licensed assets count after 90 days.

When you delete an asset, you cannot view the asset in the default view of the asset table. However, you can apply a filter to the asset table to view deleted assets.

To view deleted assets in the new interface:

1. In the upper-left corner, click the button.
   The left navigation plane appears.

2. In the left navigation plane, in the Asset View section, click Assets.
   The Assets page appears.

3. Click Filters.

4. Create a filter with the following settings:
   - Category: IsLicensed (VM)
   - Operator: is equal to
   - Value: true

5. Click Apply.
   The assets table updates to display all assets with active licenses. Deleted assets appear grayed out.
Asset Filters

You can use asset attributes to filter data in asset views and dashboards. For more information, see:

- Tenable-provided Filters
- Guidelines for Tenable-provided Filters
- Tag Filters

In Tenable.io, you can use asset filters in tables and dashboards, and to create tag rules, as follows:

<table>
<thead>
<tr>
<th>Type</th>
<th>Created By</th>
<th>Filter Tables</th>
<th>Filter Dashboards</th>
<th>Create Tag Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable-provided filters</td>
<td>Tenable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Tag filters</td>
<td>users</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Tenable-provided Filters

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Supported in Tag Rules?</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACR Score</td>
<td>(Requires Lumin license) The asset's ACR.</td>
<td>No</td>
</tr>
<tr>
<td>ACR Severity</td>
<td>(Requires Lumin license) The ACR category of the ACR calculated for the asset.</td>
<td>No</td>
</tr>
<tr>
<td>AES</td>
<td>(Requires Lumin license) The Asset Exposure Score (AES) calculated for the asset.</td>
<td>No</td>
</tr>
<tr>
<td>AES Severity</td>
<td>(Requires Lumin license) The AES category of the AES calculated for the asset.</td>
<td>No</td>
</tr>
<tr>
<td>Asset Assessed</td>
<td>Specifies whether the asset has been assessed for vulnerabilities. For a list of conditions that cause an asset to be assessed, see How Assets are Counted. Once assessed, the asset</td>
<td>Yes</td>
</tr>
<tr>
<td>Asset ID</td>
<td>The asset's UUID.</td>
<td>No</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------------------</td>
<td>----</td>
</tr>
<tr>
<td>AWS Availability Zone</td>
<td>The name of the Availability Zone where AWS hosts the virtual machine instance. For more information, see Regions and Availability Zones in the AWS documentation.</td>
<td>Yes</td>
</tr>
<tr>
<td>AWS EC2 AMI ID</td>
<td>The unique identifier of the Linux AMI image in Amazon Elastic Compute Cloud (Amazon EC2). For more information, see the Amazon Elastic Compute Cloud Documentation.</td>
<td>Yes</td>
</tr>
<tr>
<td>AWS EC2 Instance ID</td>
<td>The unique identifier of the Linux instance in Amazon EC2. For more information, see the Amazon Elastic Compute Cloud Documentation.</td>
<td>Yes</td>
</tr>
<tr>
<td>AWS EC2 Name</td>
<td>The name of the virtual machine instance in Amazon EC2.</td>
<td>Yes</td>
</tr>
<tr>
<td>AWS EC2 Product Code</td>
<td>The product code associated with the AMI used to launch the virtual machine instance in Amazon EC2.</td>
<td>Yes</td>
</tr>
<tr>
<td>AWS Instance State</td>
<td>The state of the virtual machine instance in AWS at the time of the scan. For possible values, see API Instance State in the Amazon Elastic Compute Cloud Documentation.</td>
<td>Yes</td>
</tr>
<tr>
<td>AWS Instance Type</td>
<td>The type of virtual machine instance in Amazon EC2. Amazon EC2 instance types dictate the specifications of the instance (for example, how much RAM it has). For a list of possible values, see Amazon EC2 Instance Types in the AWS documentation.</td>
<td>Yes</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>Available</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>AWS Owner</td>
<td>A UUID for the Amazon AWS account that created the virtual machine instance. For more information, see AWS Account Identifiers in the AWS documentation. This attribute contains a value for Amazon EC2 instances only. For other asset types, this attribute is empty.</td>
<td>Yes</td>
</tr>
<tr>
<td>AWS Region</td>
<td>The region where AWS hosts the virtual machine instance, for example, us-east-1. For more information, see Regions and Availability Zones in the AWS documentation.</td>
<td>Yes</td>
</tr>
<tr>
<td>AWS Security Group</td>
<td>The AWS security group (SG) associated with the Amazon EC2 instance.</td>
<td>Yes</td>
</tr>
<tr>
<td>AWS Subnet ID</td>
<td>The unique identifier of the AWS subnet where the virtual machine instance was running at the time of the scan.</td>
<td>Yes</td>
</tr>
<tr>
<td>AWS VPC ID</td>
<td>The unique identifier of the public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private Cloud User Guide.</td>
<td>Yes</td>
</tr>
<tr>
<td>Azure Resource ID</td>
<td>The unique identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.</td>
<td>Yes</td>
</tr>
<tr>
<td>Azure VM ID</td>
<td>The unique identifier of the Microsoft Azure virtual machine instance. For more information, see Accessing and Using Azure VM Unique ID in the Microsoft Azure documentation.</td>
<td>Yes</td>
</tr>
<tr>
<td>BigFix Asset ID</td>
<td>The unique identifiers of the asset in IBM BigFix. For more information, see the IBM</td>
<td>No</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Filterable</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Created Date</td>
<td>The time and date when Tenable.io created the asset record.</td>
<td>No</td>
</tr>
<tr>
<td>Deleted Date</td>
<td>The time and date when a user deleted the asset record. When a user deletes an asset record, Tenable.io retains the record until the asset ages out of the license count.</td>
<td>No</td>
</tr>
<tr>
<td>Device Type</td>
<td>(Requires Lumin license) The device_type key driver value that influenced the asset's calculated ACR score.</td>
<td>No</td>
</tr>
<tr>
<td>DNS</td>
<td>The fully-qualified domain name of the host that the vulnerability was detected on.</td>
<td>Yes</td>
</tr>
<tr>
<td>First Seen</td>
<td>The time and date when a scan first identified the asset.</td>
<td>No</td>
</tr>
<tr>
<td>Google Cloud Instance ID</td>
<td>The unique identifier of the virtual machine instance in Google Cloud Platform (GCP).</td>
<td>Yes</td>
</tr>
<tr>
<td>Google Cloud Project ID</td>
<td>The customized name of the project to which the virtual machine instance belongs in GCP. For more information, see Creating and Managing Projects in the GCP documentation.</td>
<td>Yes</td>
</tr>
<tr>
<td>Google Cloud Zone</td>
<td>The zone where the virtual machine instance runs in GCP. For more information, see Regions and Zones in the GCP documentation.</td>
<td>Yes</td>
</tr>
<tr>
<td>Has Plugin Results</td>
<td>Specifies whether the asset has plugin results associated with it.</td>
<td>Yes</td>
</tr>
<tr>
<td>Hostname/IP Address</td>
<td>Use this filter to limit assets by the following asset identifiers:</td>
<td>No</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Note</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>hostname</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FQDN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv4 address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This filter supports multiple asset identifiers as a comma-separated list</td>
<td>Note: You cannot filter assets by IPv6 address.</td>
</tr>
<tr>
<td></td>
<td>(for example, hostname_example, example.com, 192.168.0.0). For IP addresses,</td>
<td>Note: Ensure the search query does not end in a period.</td>
</tr>
<tr>
<td></td>
<td>you can specify individual addresses, CIDR notation (for example, 192.168.0.0/24), or a range (for example, 192.168.0.1-192.168.0.255).</td>
<td></td>
</tr>
<tr>
<td>Installed Software</td>
<td>A list of Common Platform Enumeration (CPE) values that represent software</td>
<td>Note: If no scan detects an application within 30 days of the scan that originally detected the</td>
</tr>
<tr>
<td></td>
<td>applications a scan identified as present on an asset. This field supports</td>
<td>application, Tenable.io considers the detection of that application expired. As a result, the</td>
</tr>
<tr>
<td></td>
<td>the CPE 2.2 format. For more information, see the Component Syntax section of</td>
<td>next time a scan evaluates the asset, Tenable.io removes the expired application from the</td>
</tr>
<tr>
<td></td>
<td>the CPE Specification documentation, Version 2.2. For assets identified in</td>
<td>Installed Software attribute. This activity is logged as a remove type of attribute change in the</td>
</tr>
<tr>
<td></td>
<td>Tenable scans, this field contains data only if a scan using Nessus Plugin</td>
<td>asset activity log.</td>
</tr>
<tr>
<td></td>
<td>ID 45590 has evaluated the asset.</td>
<td></td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>An IPv4 address that a scan has associated</td>
<td></td>
</tr>
</tbody>
</table>
This filter supports multiple asset identifiers as a comma-separated list (for example, hostname_example, example.com, 192.168.0.0). For IP addresses, you can specify individual addresses, CIDR notation (for example, 192.168.0.0/24), or a range (for example, 192.168.0.1-192.168.0.255).

**Note:** A CIDR mask of /0 is not supported for this parameter, because that value would match all IP addresses. If you submit a /0 value for this parameter, Tenable.io returns a 400 Bad Request error message.

**Note:** Ensure the search query does not end in a period.

<table>
<thead>
<tr>
<th>IPv6 Address</th>
<th>An IPv6 address that a scan has associated with the asset record. This filter supports multiple asset identifiers as a comma-separated list. The IPv6 address must be an exact match. (for example, 0:0:0:0:0:0:0:0:fff:0:0a8:0).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is Licensed (VM)</td>
<td>Specifies whether the asset is included in the asset count for the Tenable.io instance.</td>
</tr>
<tr>
<td>Is Licensed (WAS)</td>
<td>Specifies whether the asset is included in the asset count for the Tenable.io Web Application Scanning instance. An asset is licensed if it meets the following criteria:</td>
</tr>
</tbody>
</table>
- The scan results for the asset do not include discovery plugin results.

- The scan results for the asset do not include Tenable.io Web Application Scanning sources (e.g., results from Nessus scanners, Agents, Nessus Network Monitor).

- The asset has not been terminated.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is Deleted</td>
<td>Specifies whether the asset has been deleted.</td>
<td>No</td>
</tr>
<tr>
<td>Is Terminated</td>
<td>Specifies whether the virtual instance of the asset has been terminated.</td>
<td>No</td>
</tr>
<tr>
<td>Last Assessed</td>
<td>A Tenable-provided time period during which an assessment scan ran against the asset. Supported values are:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• 7 Days Ago</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 14 Days Ago</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 30 Days Ago</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 90 Days Ago</td>
<td></td>
</tr>
<tr>
<td>Last Assessed Date</td>
<td>The start date of a user-defined period during which an assessment scan ran against the asset. The implicit end date is the current date.</td>
<td>No</td>
</tr>
<tr>
<td>Last Authenticated Scan</td>
<td>The time and date of the last credentialed scan run on the asset.</td>
<td>No</td>
</tr>
</tbody>
</table>

**Note:** The following operators are supported by this filter:

- **Earlier than** – Returns any asset that meets
either of the following conditions:

- Tenable.io has never run a credentialed scan for the asset.
- The most recent credentialed scan of the asset ran earlier than 12 AM on the selected date.

For example, if, on June 15, you select the date range **30 Days Ago**, the credentialed scan must have started to run before 12 AM on May 16. In other words, the filter returns assets from May 15 or earlier.

- **Earlier than (strict)** – Returns the same assets as **Earlier than**, except that it excludes assets for which Tenable.io has never run a credentialed scan on.

- **Later than** – Returns the most recent credentialed scan of the asset. Includes only scans run later than 12 AM on the selected date.

For example, if, on June 15, you select the date range **30 Days Ago**, the credentialed scan must have started after 12 AM on May 16. In other words, the filter returns assets from May 16 or later.

<table>
<thead>
<tr>
<th>Last Seen</th>
<th>The date and time of the scan that most recently identified the asset.</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>A MAC address that a scan has associated with the asset record.</td>
<td>Yes</td>
</tr>
<tr>
<td>Mitigation</td>
<td>An umbrella filter that, when selected, filters on the following criteria:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• Mitigation - Detected: Specifies whether a</td>
<td></td>
</tr>
</tbody>
</table>
scan has identified a mitigation on the asset.

- Mitigation - Last Detected: The date range within which a scan identified a mitigation on the asset. Possible values are earlier than or later than:
  - 7 Days ago
  - 14 Days Ago
  - 30 Days Ago
  - 90 Days Ago

- Mitigation - Product Name: The name of the mitigation software identified on the asset. Lumin defines mitigations as security agent software running on endpoint assets, which include antivirus software, Endpoint Protection Platforms (EPPs), or Endpoint Detection and Response (EDR) solutions.

- Mitigation - Vendor Name: The name of the vendor for the mitigation that a scan identified on the asset.

- Mitigation - Version: The version of the mitigation that a scan identified on the asset.

<table>
<thead>
<tr>
<th>NetBIOS Name</th>
<th>The NetBIOS name for the asset.</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Name</td>
<td>The name of the network object associated with scanners that identified the asset. The default network name is <strong>Default</strong>. For more information about networks, see <a href="#">Networks</a>.</td>
<td>Yes</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Is Relevant</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Operating System</td>
<td>The operating system that a scan identified as installed on the asset.</td>
<td>Yes</td>
</tr>
<tr>
<td>Qualys Asset ID</td>
<td>The Asset ID of the asset in Qualys. For more information, see the Qualys documentation. This field contains a value only for assets associated with Qualys vulnerabilities you import via the Tenable.io API. For more information, see the Tenable Developer Portal.</td>
<td>Yes</td>
</tr>
<tr>
<td>Qualys Host ID</td>
<td>The Host ID of the asset in Qualys. For more information, see the Qualys documentation. This field contains a value only for assets associated with Qualys vulnerabilities you import via the Tenable.io API. For more information, see the Tenable Developer Portal.</td>
<td>Yes</td>
</tr>
<tr>
<td>Scan Frequency</td>
<td>The number of times the asset was scanned within the past 90 days.</td>
<td>No</td>
</tr>
<tr>
<td>ServiceNow Sys ID</td>
<td>The unique record identifier of the asset in ServiceNow. For more information, see the ServiceNow documentation.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
| Source                  | The source of the scan that identified the asset. Possible values are:  
  - Agent (Nessus Agent)  
  - Nessus (Nessus scan)  
  - PVS/NNM (Nessus Network Monitor)  
  - WAS (Web Application Scanning)  
  - AWS Connector  
  - Azure Connector                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Yes         |
<table>
<thead>
<tr>
<th>Tag (Category: Value)</th>
<th>A unique filter that searches tags (category: value) pairs. For more information, see <a href="#">tags</a>.</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Groups</td>
<td>The target group to which the asset belongs. This attribute is empty if the asset does not belong to a target group. For more information, see <a href="#">Target Groups</a>.</td>
<td>No</td>
</tr>
<tr>
<td>Tenable UUID</td>
<td>The UUID of the agent present on the asset. This attribute is empty if no agent is present on the asset.</td>
<td>Yes</td>
</tr>
<tr>
<td>Terminated Date</td>
<td>The date on which the virtual instance of the asset was terminated.</td>
<td>No</td>
</tr>
</tbody>
</table>

**Guidelines for Tenable-provided Filters**

Tenable recommends using human-readable strings when using the `contains` or `does not contain` operator for the following filters:

- ACR Drivers
- DNS (FQDN)
- Hostname/IP Address
- Installed Software
- NetBIOS Name
- Operating System

**Note:** When using the `contains` or `does not contain` operators, do not use periods in your search values. Additionally, the search values are case sensitive.
For example, when filtering on Operating System, use "Windows" instead of "Win." Tenable also recommends filtering on characters at the beginning of search strings, instead of characters in the middle or end of search strings. For example, when trying to match on an asset with the hostname "localhost", filtering on "local," instead of "host" or "h," returns better results.

Tag Filters

In Tenable.io, tags allow you to add descriptive metadata to assets that helps you group assets by business context. For more information, see Tags.

On the Assets page, you can filter vulnerabilities by tags applied to the related assets.

In the Category drop-down box for a filter, your organization's tags appear at the bottom of the list, after the Tenable-provided filters.

If you want to export vulnerabilities for assets filtered by tag, use the CSV export format. Tag filters are not supported in other export formats.

**Note:** If you exceed the current asset query limitation of 25,000, a message appears in your interface. Refine the query to a tag that returns fewer than 25,000 assets.

You can also use tag filters to create tag rules.
Assets (Classic Interface)

**Note:** This section describes the classic Tenable.io interface. For an introduction to the new interface, see Assets.

Tenable.io includes the ability to track assets that belong to your organization. Assets are entities of value on a network that can be exploited. This includes laptops, desktops, servers, routers, mobile phones, virtual machines, software containers, and cloud instances. By providing comprehensive information about the assets that belong to your organization, Tenable.io helps to eliminate potential security risks, identify under-utilized resources, and support compliance efforts.

Tenable.io automatically creates or updates assets when a scan completes or scan results are imported. Tenable.io attempts to match incoming scan data to existing assets using a complex algorithm. This algorithm looks at attributes of the scanned hosts and employs a variety of heuristics to choose the best possible match. If Tenable.io cannot find a match, the system assumes this is the first time Tenable.io has encountered the asset and creates a new record for it. Otherwise, if Tenable.io finds a matching asset, the system updates any properties that have changed since the last time Tenable.io encountered the asset.

In addition to vulnerability information, Tenable.io also attempts to gather various other information about the asset, including:

- Interfaces (IP address and MAC address)
- DNS Names
- NetBIOS Name
- Operating System
- Installed Software
- UUIDS (Tenable, ePO, BIOS)
- Whether an agent is present

When you access the Assets workbench, a table of assets appears. This documentation refers to that table as the *assets table*. When you view an asset on the assets table, or directly via the Assets workbench, you can view the Tenable agents that observed the asset, the date it was discovered, and the date it was last observed. You can also view additional information about the asset.
When you view an asset, the **Vulnerabilities** section appears, displaying a table of vulnerabilities. The **Vulnerabilities** section is identical to the [information you can view using the Vulnerabilities workbench](#), but filtered to vulnerabilities detected on the selected asset.
Manage Assets (Classic Interface)

To access the Assets dashboard:

1. In the top navigation bar, click **Dashboards**.
   
   Your default dashboard appears. If you have not set a default dashboard, the **Vulnerabilities** workbench appears.

2. In the left navigation bar, click **Assets**.
   
   The Assets dashboard appears, and displays the assets table.

3. In the Assets dashboard, do any of the following:
   
   - [Search and filter assets](#)
   - [View vulnerability information for assets](#)
   - [Export vulnerability data for assets](#)
   - [View additional information about assets](#)
   - [Manage asset tags](#)
   - [Delete assets](#)
   - [View deleted assets](#)
Search and Filter Assets (Classic Interface)

At the top of the **Assets** page, you can search and filter through your assets in Tenable.io. The simple **Search** bar searches only the first 5,000 records initially displayed. The **Advanced** search searches through all records and returns up to 5,000 matching records.
View Asset Vulnerabilities (Classic Interface)

To view vulnerabilities for a specific asset:

1. In the top navigation bar, click **Dashboards**.
   
   Your default dashboard appears. If you have not set a default dashboard, the **Vulnerabilities** workbench appears.

2. In the left navigation bar, click **Assets**.

   The **Assets** dashboard appears, and displays the assets table.

3. Click the name of the asset that has vulnerabilities you want to view.

   The **Overview** tab for the asset appears.

4. Click the **Vulnerabilities** tab.

5. In the table of vulnerabilities, click the vulnerability for which you want to view more information.

   The plugin details page appears.
View Additional Asset Information (Classic Interface)

To view additional information about an asset:

1. In the top navigation bar, click **Dashboards**.
   
   Your default dashboard appears. If you have not set a default dashboard, the **Vulnerabilities** workbench appears.

2. In the left navigation bar, click **Assets**.
   
   The **Assets** dashboard appears, and displays the assets table.

3. Click the name of the asset where you want to view additional information.
   
   The **Overview** tab for the asset appears.

4. Click the **Additional Info** tab.
   
   The **Additional Info** section appears, displaying information about agents, IP addresses, DNS entries, MAC addresses, and operating systems associated with the asset.
Delete Assets (Classic Interface)

You can delete assets as a standard or administrative user.

When you delete an asset, Tenable.io:

- removes the asset from the default view of the assets table.
- deletes vulnerability data associated with the asset.
- stops matching scan results to the asset.

Deleting an asset does not immediately subtract the asset from your licensed assets count. Deleted assets continue to be included in the count until they automatically age out of your licensed assets count after 90 days.

You cannot reverse the deletion of an asset. If you mistakenly delete an asset, add it to the system by scanning the asset again.

For more information, see:

- [Delete Assets from the Assets Table (Classic Interface)](#)
- [Delete Assets from the Asset Detail Page (Classic Interface)](#)
- [View Deleted Assets (Classic Interface)](#)
Delete Assets from the Assets Table (Classic Interface)

To delete assets from the assets table on the **Assets** dashboard:

1. In the top navigation bar, click **Dashboards**.
   
   Your default dashboard appears. If you have not set a default dashboard, the **Vulnerabilities** workbench appears.

2. In the left navigation bar, click **Assets**.
   
   The **Assets** dashboard appears, and displays the assets table.

3. To delete one asset, click the ✗ button next to the asset you want to delete.
   
   -or-

   To delete multiple assets:
   
   a. Select the check box next to each asset you want to delete.
   
   b. Click **Delete** in the upper right corner of the page.

4. Click **Delete** to confirm the deletion.

   The system marks the asset or assets deleted.
Delete Assets from the Asset Detail Page (Classic Interface)

To delete assets from the Asset Detail page:

1. In the top navigation bar, click **Dashboards**.
   
   Your default dashboard appears. If you have not set a default dashboard, the **Vulnerabilities** workbench appears.

2. In the left navigation bar, click **Assets**.
   
   The **Assets** dashboard appears, and displays the assets table.

3. In the assets table, click the asset you want to delete.
   
   The assets detail page appears.

4. Click **Delete** in the upper right corner.

5. Click **Delete** again to confirm.

   The system marks the asset deleted.
View Deleted Assets (Classic Interface)

You can view information about deleted assets until they age out of your licensed assets count as inactive after 90 days.

In the assets table on the **Assets** dashboard, deleted assets are grayed out and labeled as deleted.

In the asset detail page, you can view deleted asset details on the **Overview** and **Additional Info** tabs, but the **Vulnerabilities** tab is empty, because Tenable.io does not retain vulnerabilities data for deleted assets.

To view deleted assets:

1. In the top navigation bar, click **Dashboards**.
   
   Your default dashboard appears. If you have not set a default dashboard, the **Vulnerabilities** workbench appears.

2. In the left navigation bar, click **Assets**.

   The **Assets** dashboard appears, and displays the assets table.

3. In the top navigation bar, click the **Advanced** search button.

4. In the **Match** drop-down box, click **Any** to view results that match any of the filters you create, or click **All** to view results that match all of the filters you create.

5. Set the **Is Licensed** filter equal to **true**.

6. Click **Apply**.
Manage Asset Tags (Classic Interface)

Video: Categorizing Assets with Tags in Tenable.io

You can manage asset tags in any user role.

In the Assets dashboard of Tenable.io, you can manage tags for your assets. You can:

- Apply tags to an individual asset or multiple assets
- Remove tags applied to an individual asset or multiple assets
- Create tag rules from advanced search filters

Tip: Applying or removing a tag generates an entry in the asset's activity log. You can view the activity log in the Overview tab of the asset details.

Note: Tenable.io applies dynamic tags to any assets, regardless of access group scoping. As a result, it may apply tags you create to assets outside of access groups to which you belong.

When applying tags to assets, you can select from existing tags or create new tags.

After applying tags to assets, you can filter assets by tag.

Note: This section of the documentation describes tag management in the Dashboards page. For more information on creating and modifying tags in the Settings page, see Tags.
Apply a Tag to an Asset (Classic Interface)

Required Tenable.io Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Note: When you apply a tag to an asset manually, Tenable.io excludes that asset from any further evaluation against the tag's rules. The tag remains applied to the asset despite changes to the asset's attributes or the tag rules. To restore automatic tag evaluations for that asset, remove the manually-applied tag from the asset, then remove the asset from the Excluded Assets list for the tag.

To apply a tag to an asset:

1. In the top navigation bar, click Dashboards.

   Your default dashboard appears. If you have not set a default dashboard, the Vulnerabilities workbench appears.

2. In the left navigation bar, click Assets.

   The Assets dashboard appears, and displays the assets table.

3. To apply a tag to an asset(s), using one of the following methods:

   **Apply a tag to one asset in the assets table.**
   
   a. In the assets table, click the ••• button next to the asset where you want to apply a tag
   
   b. Click Add Tags in the menu.

   -or-

   **Apply a tag to multiple assets in the assets table.**
   
   a. In the assets table, select the check box next to each asset where you want to apply the tag.
   
   b. Click the Add Tags button in the upper right corner of the page.

   -or-

   **Apply a tag to one asset on the asset detail page.**
a. Click the name of the asset where you want to add a tag.
   
   The asset detail page appears. The **Overview** tab displays a **Tags** section.

b. Click the button next to the **Tags** header.

4. In the **Add Tags** window, select tags using any of the following methods:

Search for an existing tag.

a. Select an existing category from the **Category** drop-down list.

b. Select an existing tag from the **Value** drop-down list.

c. Click the button. The tag appears in the **TAGS TO BE ADDED** box.

-or-

Create a new tag and tag category.

a. Type a new category name in the **Category** box.

b. Click **Create New "name" Category**.

c. Type a new tag value in the **Value** box.

   **Note:** Tag values cannot include commas.

d. Click **Create New "value" Value**.

e. Click the button. The new tag appears in the **TAGS TO BE ADDED** box.

   **Note:** The system does not save tags you add by this method unless you apply the new tags to the asset at the same time.

-or-

Add a new tag to an existing tag category.

a. Select an existing category from the **Category** drop-down list.

b. Type a new tag value in the **Value** box.

c. Click **Create New "value" Value**.
d. Click the + button. The new tag appears in the **TAGS TO BE ADDED** box.

**Note:** The system does not save tags you add by this method unless you apply the new tags to the asset at the same time.

-or-

Click any tag in the **RECENTLY USED TAGS** box. The tag appears in the **TAGS TO BE ADDED** box.

5. Click **Add**.

Tenable.io applies the tags you selected to the asset or assets you selected.

If you created a new tag or tag category during the tag selection, Tenable.io saves that tag or category. You can now apply the tag to additional assets and view it in the tags table under **Settings**.
Remove a Tag from an Asset (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Note:** If you remove a dynamic tag from an asset, Tenable.io excludes the asset from further evaluations against the tag's rules. To restore automatic tag evaluations for that asset, remove the asset from the Excluded Assets list for the tag. For more information, see Edit Tag Rules.

To remove a tag from an asset in the classic interface:

### Remove a Tag in the Assets Table

1. In the top navigation bar, click **Dashboards**.
   
   Your default dashboard appears. If you have not set a default dashboard, the **Vulnerabilities** workbench appears.

2. In the left navigation bar, click **Assets**.
   
   The **Assets** dashboard appears, and displays the assets table.

3. To remove tags from one asset, click the 
   
   To remove tags from multiple assets:

   - Select the check box next to the assets where you want to remove tags.
   - In the upper right corner of the page, click **Remove Tags**.

   The **Remove Tags** window appears. The tags currently applied to the asset or assets display in the **CURRENT TAGS** box.

4. Click any tag in the **CURRENT TAGS** box to add it to the **TAGS TO BE REMOVED** box.

5. Click **Remove**.

   The **Confirm Changes** window appears.

6. Click **Remove** to confirm the removal.
The system removes the tags you selected from the asset or assets you selected.

Remove a Tag on the Asset Detail Page

1. In the top navigation bar, click **Dashboards**.
   
   Your default dashboard appears. If you have not set a default dashboard, the **Vulnerabilities** workbench appears.

2. In the left navigation bar, click **Assets**.

   The **Assets** dashboard appears, and displays the assets table.

3. Click the name of the asset where you want to remove tags.

   The asset detail page appears. The **Overview** tab displays the **Tags** section.

4. Click any tag in the **Tags** section.

5. Click **Remove Tag** in the menu.

   The **Confirm Changes** window appears.

6. Click **Remove** to confirm the removal.

   Tenable.io removes the tag you selected from the asset.
Create Tag Rules from Advanced Search Filters (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can configure advanced search filters in the **Assets** dashboard, then save those filters as **tag rules**.

To create an asset tag rule from an advanced search filter in the classic interface:

1. In the top navigation bar, click **Dashboards**.
   
   Your default dashboard appears. If you have not set a default dashboard, the **Vulnerabilities** workbench appears.

2. In the left navigation bar, click **Assets**.
   
   The **Assets** dashboard appears, and displays the assets table.

3. In the top navigation bar, click the **Advanced** search button.
   
   The **Advanced Search** window appears.

4. Select the filters for your search.

5. Click the **button in the upper right corner of the window.
   
   The **Create Tag** window appears.

6. To add a new category, type a category name in the **Category** box.
   
   -or-  
   
   To use an existing category for the tag, select a category from the drop-down box.

   **Note:** This field is required. If you want to create tags without individual categories, Tenable recommends that you add the generic category **Category**, which you can use for all your tags.

7. Type a tag value in the **Value** box.

8. (Optional) In the **Category Description** box, type a description of the tag category.
9. (Optional) In the **Value Description** box, type a description for the new tag value.

10. Verify that the elements of your advanced search filter are present as tag rules.

11. Click **Create**.
Filter the Assets Workbench by Tag (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Note:** This topic describes searching and filtering by tags in the assets workbench. For more information on filtering by tags from the Settings page, see Search Assets by Tag in the Tags Table.

To filter the assets workbench by tag in the classic interface:

**Filter Assets by Tag in the Assets Table**

1. In the top navigation bar, click **Dashboards**.
   
   Your default dashboard appears. If you have not set a default dashboard, the **Vulnerabilities** workbench appears.

2. In the left navigation bar, click **Assets**.
   
   The **Assets** dashboard appears, and displays the assets table.

3. Click **Advanced** next to the search box in the top navigation bar.
   
   The **Advanced Search** window appears.

4. Select **All** in the match drop-down box to return assets that meet all the filter criteria you specify.
   
   -or-

   Select **Any** in the match drop-down box to return assets that meet any of the criteria you specify.

5. Select a tag category in the filter drop-down box.
   
   Asset tags appear in the **Tags** section of the list.

6. Select an operator from the operator drop-down box.

7. Select a tag value from the value drop-down box.

8. (Optional) Click the button next to the filter you added to add other filters to your search.
9. Click **Apply**.

   The assets table displays assets that meet the filter criteria you specified. For more information, see [Search and Filter Assets (Classic Interface)](#).

**Filter Assets by Tag from the Asset Detail Page**

1. In the top navigation bar, click **Dashboards**.

   Your default dashboard appears. If you have not set a default dashboard, the **Vulnerabilities** workbench appears.

2. In the left navigation bar, click **Assets**.

   The **Assets** dashboard appears, and displays the assets table.

3. Click the name of the asset where you want to view details.

   The asset detail page appears. The **Overview** tab displays the **Tags** section.

4. Click any tag in the **Tags** section.

5. Click **Search Assets by Tag**.

   The **Assets** dashboard appears. The assets table contains only assets where the tag you selected is applied.

   **Tip:** To remove this filter or filter by another tag, click **Advanced** in the top navigation bar and change the filter. For more information, see [Search and Filter Assets](#).
Vulnerabilities

**Note:** This section describes the new interface. For information about the classic interface, see [Vulnerabilities (Classic Interface)](Vulnerabilities_Classic_Interface). For information about navigating the new interface, see [Navigate Tenable.io (New Interface)](Navigate_Tenable.io_New_Interface).

This page contains top-level widgets that provide a snapshot of the vulnerabilities on your assets as well as a table that lists vulnerabilities that scans have identified in your network. The top-level widgets include:

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Priority Rating by Total Instances</td>
<td>This widget summarizes the number of vulnerabilities on your network, organized by VPR. For more information, see <a href="CVSS_vs_VPR">CVSS vs. VPR</a>. To view a list of vulnerabilities filtered by a VPR range, click one of the tiles. For more information, see <a href="View_Vulnerabilities_by_Plugin">View Vulnerabilities by Plugin</a>.</td>
</tr>
<tr>
<td>Unique Vulnerability by State</td>
<td>This widget summarizes vulnerabilities by New, Active, Fixed, and Resurfaced state.</td>
</tr>
<tr>
<td>Vulnerability Instance by Age</td>
<td>This widget summarizes vulnerability instances based on the selected date range.</td>
</tr>
</tbody>
</table>

The **Vulnerabilities** page provides insight into your organization's vulnerabilities and the assets where scans found the vulnerabilities. The **Vulnerabilities** page displays vulnerabilities grouped by **plugin** and by **asset**.

In the Tenable.io Web Application Scanning interface, you can also view vulnerabilities grouped by **application**.

For more information, see:

- [CVSS vs. VPR](CVSS_vs_VPR)
- [View Vulnerabilities by Plugin](View_Vulnerabilities_by_Plugin)
- [View Vulnerabilities by Asset](View_Vulnerabilities_by_Asset)
- [View Vulnerability Details](View_Vulnerability_Details)
- [Create a Recast Rule from Vulnerability Details](Create_a_Recast_Rule_from_Vulnerability_Details)
• Create an Accept Rule from Vulnerability Details

• Export Vulnerability Data

• View Plugin Output

• Copy Plugin Output

• Vulnerability Filters

• Application Filters

• Vulnerability Severity Indicators

• Vulnerability States
CVSS vs. VPR

Tenable uses CVSS scores and a dynamic Tenable-calculated Vulnerability Priority Rating (VPR) to quantify the risk and urgency of a vulnerability.

**Note:** When you view these metrics on an analysis page organized by plugin (for example, the **Vulnerabilities by Plugin** page), the metrics represent the highest value assigned or calculated for a vulnerability associated with the plugin.

For Lumin-specific information about VPR and the other Lumin metrics, see [Lumin Metrics](#).

CVSS

Tenable uses and displays third-party Common Vulnerability Scoring System (CVSS) values retrieved from the National Vulnerability Database (NVD) to describe risk associated with vulnerabilities. CVSS scores power a vulnerability’s **Severity** and **Risk Factor** values.

**Tip:** **Risk Factor** and **Severity** values are unrelated; they are calculated separately.

Tenable.io imports a CVSS score every time a scan sees a vulnerability.

CVSS-Based Severity

Tenable assigns all vulnerabilities a severity (**Info**, **Low**, **Medium**, **High**, or **Critical**) based on the vulnerability's static CVSSv2 or CVSSv3 score, depending on your configuration. For more information, see [Configure Your Severity Metric](#).

Tenable.io analysis pages provide summary information about vulnerabilities using the following CVSS categories. For more information about the icons used for each severity, see [Vulnerability Severity Indicators](#).

<table>
<thead>
<tr>
<th>Severity</th>
<th>CVSSv2 Range</th>
<th>CVSSv3 Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>The plugin's highest vulnerability CVSSv2 score is 10.0.</td>
<td>The plugin's highest vulnerability CVSSv3 score is between 9.0 and 10.0.</td>
</tr>
<tr>
<td>High</td>
<td>The plugin's highest vulnerability CVSSv2 score is between 7.0 and 10.0.</td>
<td>The plugin's highest vulnerability CVSSv3 score is between 7.0 and 8.9.</td>
</tr>
<tr>
<td>Level</td>
<td>Description</td>
<td>CVSSv2 Score</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Medium</td>
<td>The plugin's highest vulnerability CVSSv2 score is between 4.0 and 6.9.</td>
<td>The plugin's highest vulnerability CVSSv3 score is between 4.0 and 6.9.</td>
</tr>
<tr>
<td>Low</td>
<td>The plugin's highest vulnerability CVSSv2 score is between 0.1 and 3.9.</td>
<td>The plugin's highest vulnerability CVSSv3 score is between 0.1 and 3.9.</td>
</tr>
<tr>
<td>Info</td>
<td>The plugin's highest vulnerability CVSSv2 score is 0. - or - The plugin does not search for vulnerabilities.</td>
<td>The plugin's highest vulnerability CVSSv3 score is 0. - or - The plugin does not search for vulnerabilities.</td>
</tr>
</tbody>
</table>

**CVSS-Based Risk Factor**

For each plugin, Tenable interprets the CVSSv2 scores for the vulnerabilities associated with the plugin and assigns an overall risk factor (Low, Medium, High, or Critical) to the plugin. The Vulnerability Details page displays the highest risk factor value for all of the plugins associated with a vulnerability.

**Tip:** Info plugins receive a risk factor of None. Other plugins without associated CVSSv2 scores receive a custom risk factor based on information provided in related security advisories.

**Vulnerability Priority Rating**

**Video:** Vulnerability Priority Rating in Tenable.io

Tenable calculates a dynamic VPR for most vulnerabilities. The VPR is a dynamic companion to the data provided by the vulnerability's CVSS score, since Tenable updates the VPR to reflect the current threat landscape. VPR values range from 0.1-10.0, with a higher value representing a higher likelihood of exploit.
<table>
<thead>
<tr>
<th>VPR Category</th>
<th>VPR Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>9.0 to 10.0</td>
</tr>
<tr>
<td>High</td>
<td>7.0 to 8.9</td>
</tr>
<tr>
<td>Medium</td>
<td>4.0 to 6.9</td>
</tr>
<tr>
<td>Low</td>
<td>0.1 to 3.9</td>
</tr>
</tbody>
</table>

**Note:** Vulnerabilities without CVEs in the National Vulnerability Database (NVD) (e.g., many vulnerabilities with the Info severity) do not receive a VPR. Tenable recommends remediating these vulnerabilities according to their CVSS-based severity.

**Note:** You cannot edit VPR values.

Tenable.io provides a VPR value the first time you scan a vulnerability on your network. Then, Tenable.io automatically provides new and updated VPR values daily.

Tenable recommends resolving vulnerabilities with the highest VPRs first. You can view VPR scores and summary data in:

- The Tenable-provided [Vulnerability Management Overview](#) dashboard
- The [Vulnerabilities by Plugin](#) plane
- The [Vulnerabilities by Plugin (Classic)](#) page

**VPR Key Drivers**

You can view the following key drivers to explain a vulnerability's VPR.

**Note:** Tenable does not customize these values for your organization; VPR key drivers reflect a vulnerability's global threat landscape.

<table>
<thead>
<tr>
<th>Key Driver</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age of Vuln</td>
<td>The number of days since the National Vulnerability Database (NVD) published the vulnerability.</td>
</tr>
<tr>
<td>CVSSv3 Impact Score</td>
<td>The NVD-provided CVSSv3 impact score for the vulnerability. If the NVD did not provide a score, Tenable.io displays a Tenable-predicted score.</td>
</tr>
</tbody>
</table>
Exploit Code Maturity  | The relative maturity of a possible exploit for the vulnerability based on the existence, sophistication, and prevalence of exploit intelligence from internal and external sources (e.g., Reversinglabs, Exploit-db, Metasploit, etc.). The possible values (High, Functional, PoC, or Unproven) parallel the CVSS Exploit Code Maturity categories.

Product Coverage | The relative number of unique products affected by the vulnerability: Low, Medium, High, or Very High.

Threat Sources | A list of all sources (e.g., social media channels, the dark web, etc.) where threat events related to this vulnerability occurred. If the system did not observe a related threat event in the past 28 days, the system displays No recorded events.

Threat Intensity | The relative intensity based on the number and frequency of recently observed threat events related to this vulnerability: Very Low, Low, Medium, High, or Very High.

Threat Recency | The number of days (0-730) since a threat event occurred for the vulnerability.

 Threat Event Examples

Common threat events include:

- An exploit of the vulnerability
- A posting of the vulnerability exploit code in a public repository
- A discussion of the vulnerability in mainstream media
- Security research about the vulnerability
- A discussion of the vulnerability on social media channels
- A discussion of the vulnerability on the dark web and underground
- A discussion of the vulnerability on hacker forums
View Vulnerabilities by Plugin

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Access Group Permissions:** Can View

**Note:** By default, Tenable.io does not filter for informational level plugin IDs. For more information, see the knowledge base article.

To view vulnerabilities by plugin in the new interface:

1. In the upper-left corner, click the menu button.
   
   The left navigation plane appears.

2. Do one of the following:

   View Tenable.io Vulnerability Management vulnerabilities:
   
   a. In the left navigation plane, in the **Vulnerability Management** section, click **Vulnerabilities**.
      
      The **Vulnerabilities** page appears.
      
      By default, this page displays the **By Plugin** tab. The tab contains the plugins table. The plugins table lists plugins by decreasing **severity**.

   b. From this page, you can:
      
      • View information about each vulnerability in the table:
        
        • **Severity** — The vulnerability's CVSS-based severity. For more information, see [CVSS vs. VPR](#).
        
        • **Name** — The name of the plugin that identified the vulnerability.
        
        • **Plugin ID** — The ID of the plugin that identified the vulnerability.
- Family — The family of the plugin that identified the vulnerability.

- Count — The number of vulnerability instances.

**Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

- VPR — The VPR Tenable calculated for the vulnerability.

- CVSS — The CVSSv2 or CVSSv3 score associated with the vulnerability. For more information, see CVSS vs. VPR.

- Refine the data in the plugins table. For more information, see Tenable.io Tables.

- Create, edit, or apply a saved search.

**Note:** If you apply a saved search in the By Plugins tab, Tenable.io also applies the saved search to the By Assets tab.

- View the number of plugin results, next to the Search box.

- Export data for a specific plugin.

- View vulnerability details.

View Tenable.io Web Application Scanning vulnerabilities:

a. In the left navigation plane, in the Web App Scanning section, click Vulnerabilities.

The Vulnerabilities page appears.

By default, this page displays the By Plugin tab. The tab contains the plugins table. The plugins table lists plugins by decreasing severity.

b. From this page, you can:

- Filter the plugins table by vulnerability attributes.

- Search the plugins table.

- View the number of plugin results, next to the Search box.

- View vulnerability details.
View Vulnerabilities by Asset

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Access Group Permissions:** Can View

To view vulnerabilities by asset in the new interface:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Vulnerability Management** section, click **Vulnerabilities**.

   The **Vulnerabilities** page appears.

3. In the page header, click **By Asset**.

   The **By Asset** tab appears. This tab contains the assets table.

4. On this page, you can:
   - Refine the data in the assets table. For more information, see [Tenable.io Tables](#).
   - Apply a saved search to the table.
   - View the number of assets in the table, next to the **Search** box.
   - Export vulnerabilities identified on assets.
   - Add and remove asset tags.
   - Delete an asset.
   - View asset details.
   - View asset activity.
View Vulnerabilities by Application in WAS

**Required Additional License:** Tenable.io Web Application Scanning

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Access Group Permissions:** Can View

To view vulnerabilities by plugin in the new interface:

1. In the upper-left corner, click the ☐️ button.
   
   The left navigation plane appears.

2. In the left navigation plane, in the **Web App Scanning** section, click **Vulnerabilities**.
   
   The **Vulnerabilities** page appears.

3. Click the **By Application** tab.
   
   The **By Application** tab appears. This tab contains the applications table.

4. From this page, you can:
   
   - **Filter** the applications table by application attributes.
   
   - **Search** the applications table.
   
   - View the number of application results, next to the **Search** box.
   
   - View application details.
View Vulnerability Details

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Access Group Permissions:** Can View

To view vulnerability details in the new interface:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Vulnerability Management** section, click **Vulnerabilities**.

   The **Vulnerabilities** page appears.

   By default, this page displays the **By Plugin** tab. The tab contains the plugins table. The plugins table lists plugins by decreasing **severity**. By default, this page displays the **By Plugin** tab. The plugins table lists plugins by decreasing **severity**.

3. (Optional) Refine the plugins listed in the table. For more information, see [Tenable.io Tables](#).

4. In the plugins table, click the plugin where you want to view details.

   The **Vulnerability Details** page appears.
Vulnerability Details

On the **Vulnerability Details** page, you can do the following:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right section</td>
<td></td>
</tr>
<tr>
<td><strong>Plugin Details</strong></td>
<td>View information about the plugin that identified the vulnerability. Details include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Publication Date</strong> – The date on which the plugin that identified the vulnerability was published.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Modification Date</strong> – The date on which the plugin was last modified.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Family</strong> – The family of the plugin that identified the vulnerability.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong> – The general type of plugin check (for example, local or remote).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Plugin ID</strong> – The ID of the plugin that identified the vulnerability.</td>
</tr>
<tr>
<td><strong>Exploitability Information</strong></td>
<td>View information about the vulnerability when the Exploit Available filter is applied. See <a href="#">Vulnerability Filters</a> for more information.</td>
</tr>
<tr>
<td><strong>Discovery</strong></td>
<td>View information about when the vulnerability was discovered. Details include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>First Seen</strong> – The date when a scan first found the vulnerability on an asset.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Last Seen</strong> – The date when a scan last found the vulnerability on an asset.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Age</strong> – The number of days since a scan first found the vulnerability on an asset in your network.</td>
</tr>
<tr>
<td><strong>VPR Key Drivers</strong></td>
<td>View details about the key drivers Tenable used to calculate a VPR for the vulnerability. For more information about VPR key drivers, see <a href="#">CVSS vs. VPR</a>.</td>
</tr>
<tr>
<td>Risk Information</td>
<td>View information about the risk that the vulnerability poses to your network. Details include:</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• <strong>Vulnerability Priority Rating (VPR)</strong> – The VPR Tenable calculated for the vulnerability.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Risk Factor</strong> – The CVSS-based risk factor associated with the plugin.</td>
</tr>
<tr>
<td></td>
<td>• <strong>CVSS Base Score</strong> – The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).</td>
</tr>
<tr>
<td></td>
<td>• <strong>CVSS Vector</strong> – The raw CVSSv2 metrics for the vulnerability. For more information, see CVSSv2 documentation.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <a href="#">CVSS vs. VPR</a>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vulnerability Information</th>
<th>View information about the vulnerability that the plugin identified. Details include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>Vuln Published</strong> – The date when the vulnerability definition was first published (for example, the date that the CVE was published).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Exploitation</strong> – Characteristics of the vulnerability that factor into its potential exploitability. Roll over the exploitability icons to view descriptions of characteristics.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Patch Published</strong> – The date on which the vendor published a patch for the vulnerability.</td>
</tr>
<tr>
<td></td>
<td>• <strong>CPE</strong> – The Common Platform Enumeration (CPE) numbers for vulnerabilities that the plugin identifies.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reference Information</th>
<th>View a list of references to third-party information about the vulnerability, exploit, or update associated with the plugin. Details include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>CVE</strong> – Link to external documentation of a CVE that the plugin identifies.</td>
</tr>
<tr>
<td>Upper-right corner</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td></td>
</tr>
<tr>
<td>Date range selector</td>
<td>Change the date range for data showing on the tabs. For more information, see <a href="#">Tenable.io Tables</a>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bottom section</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assets Affected</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Output</strong></td>
</tr>
</tbody>
</table>
When you access the **Vulnerability Details** page, this tab is active by default.

Details on this tab include:

- **Description** — The description of the Tenable plugin that identified the vulnerability.

- **Solution** — A brief summary of how you can remediate the vulnerability.

- **See Also** — Links to external websites that contain helpful information about the vulnerability.

- **Output** — The text output of the Nessus scanner that identified the vulnerability.

**Note:** Output for an individual plugin is limited to 1,024 KB (1 MB).

In the **Output** section of the **Details** tab, you can:

- **Export** vulnerability instance data.

- **Copy** plugin output to your computer’s clipboard.

- **View** plugin attachments.

- **Launch** a remediation scan for the vulnerability on one or more assets.

- Click a row in the vulnerability instances table to view **asset details**.
Create an Accept Rule from Vulnerability Details

**Required User Role:** Administrator

**Required Access Group Permissions:** Can View

Accept rules can be created via the Settings page, or via the Vulnerability Details page.

To create an accept rule via the Vulnerability Details page:

1. View the Vulnerability Details page.

2. In the Assets Affected table, select the check box(es) next to the asset(s) for which you want to create an accept rule.

3. In the upper-right corner, click the Actions button.

   The actions menu appears.

4. In the actions menu, click Recast.

   The Recast Rule plane appears.

5. In the Action section, select Accept.

6. In the Vulnerability section, confirm the plugin ID populated by Tenable.io.

7. In the Targets section, confirm the target populated by Tenable.io. For example:
   
   - If you select all assets on the Vulnerability Details page, the target is set to All.
   
   - If you select only some of the assets on the Vulnerability Details page, the target is set to Custom.

8. (Optional) In the Expires box, set an expiration date for the rule.

   This action is only necessary if you want the rule to expire. By default, the rule applies indefinitely.

9. (Optional) In the Comments box, type a description of the rule. The text you type in this box is only visible if the rule is modified and has no functional effect.
10. (Optional) To report the vulnerability as a false positive:
   a. Enable the **Report as false positive** toggle.
      
      A **Message To Tenable** box appears.
   b. In the **Message to Tenable** box, type a description of the false positive to send to Tenable.

11. Click **Save**.

    Tenable.io starts applying the rule to the appropriate vulnerabilities. This process may take some time, depending on the system load and the number of matching vulnerabilities. The affected vulnerability is hidden on your dashboards.

    **Note:** To view vulnerabilities hidden from your dashboards, use the **Recast & Accept** filter.
Create a Recast Rule from Vulnerability Details

**Required User Role:** Administrator

**Required Access Group Permissions:** Can View

Recast rules can be created via the Settings page, or via the Vulnerability Details page.

To create a recast rule via the Vulnerability Details page:

1. View the Vulnerability Details page.

2. In the Assets Affected table, select the check box(es) next to the asset(s) for which you want to create a recast rule.

3. In the upper-right corner, click the Actions button.
   
   The actions menu appears.

4. In the actions menu, click Recast.

   The Recast Rule plane appears.

5. In the Action section, select Recast.

6. In the Vulnerability section, confirm the plugin ID populated by Tenable.io.

7. From the New Severity drop-down box, select the severity level for the vulnerability.

8. In the Targets section, confirm the target populated by Tenable.io. For example:

   - If you select all assets on the Vulnerability Details page, the target is set to All.

   **Note:** If the Targets drop-down is set to All, a warning appears indicating that this option may override existing rules.

   - If you select only some of the assets on the Vulnerability Details page, the target is set to Custom, and Tenable.io populates the Target Hosts box with the appropriate targets.

9. (Optional) In the Expires box, set an expiration date for the rule.

   This action is only necessary if you want the rule to expire. By default, the rule applies indefinitely.
10. (Optional) In the **Comments** box, type a description of the rule.

   The text you type in this box is only visible if the rule is modified and has no functional effect.

11. Click **Save**.

   Tenable.io starts applying the rule to the appropriate vulnerabilities. This process may take some time, depending on the system load and the number of matching vulnerabilities. The change is reflected on dashboards, where a label appears to indicate how many instances of affected vulnerabilities have been recast.

   **Note:** A recast rule does not affect the historical results of a scan.
View Plugin Output

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Access Group Permissions:** Can View

**Note:** Output for an individual plugin is limited to 1,024 KB (1 MB).

To view plugin output:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, in the **Vulnerability Management** section, click **Vulnerabilities**.
   
   The **Vulnerabilities** page appears.
   
   By default, this page displays the **By Plugin** tab. The tab contains the plugins table. The plugins table lists plugins by decreasing severity.

3. (Optional) Refine the plugins listed in the table. For more information, see [Tenable.io Tables](#).

4. In the vulnerabilities table, click the vulnerability where you want to view details.
   
   The **Vulnerability Details** page appears.

5. In the **Output** section of the **Details** tab, view the plugin output.
   
   **Note:** Output for an individual plugin is limited to 1,024 KB (1 MB).

6. (Optional) Copy the plugin output to your computer's clipboard.
Copy Plugin Output

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Access Group Permissions:** Can View

**Note:** Output for an individual plugin is limited to 1,024 KB (1 MB).

To copy the plugin output for a vulnerability instance:

1. View the vulnerability details.
2. In the **Output** section of the **Details** tab, locate the box for the plugin output you want to copy.
3. In the upper-right corner of a plugin output box, click the button.

   Tenable.io copies the output to your computer's clipboard. A confirmation message appears.
View Plugin Attachments

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Scan Permissions:** Can View

Certain plugins include attachments that provide more details about specific vulnerabilities. For example, Plugin ID 92365 collects the hosts file from a remote host. After a scan is complete, you can view and save the attachment.

**Note:** Not all vulnerability output details include attachments.

To view plugin attachments for Vulnerability Management scans:

1. View individual scan details for a scan that includes plugin attachments.
2. On the **Vulns by Plugin** tab, click a vulnerability row with a plugin that includes attachments.
   
   The **Vulnerability Details** page appears.
3. Click the **Output** tab.
4. In the output table, in the row for the plugin that includes attachments, click the button.
   
   The attachment plane appears. This plane contains a table that lists available attachments.
5. In the attachments table, click the attachment you want to view.
   
   The attachment contents appear in a new browser tab.

To view plugin attachments for web application scans:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.
2. In the left navigation plane, in the **Web App Scanning** section, click **Scans**.
The Web Application Scanning **Scans** page appears.

**Note:** If your Tenable.io Web Application Scanning license expires, your web application scans no longer appear in the scans table.

3. In the scans table, click the scan that has a plugin attachment you want to view.

   The **Scan Details** page appears.

4. In the **Vulns by Plugin** tab, click the plugin you want to view.

   The **Vulnerability Details** page appears.

5. Click the **Instances** tab.

   A list of instances found for that plugin appears, categorized by URL.

6. Click the instance that has attachments you want to include.

   The instance details plane appears.

7. In the instance details plane, click the **Attachments** tab.

   The attachments table appears.

   **Note:** The **Attachments** tab appears only if the plugin instance includes an attachment.

8. Click the attachment you want to view.

   The attachment opens as a .png image or complete HTTP web page.
Export Vulnerability Data

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Access Group Permissions:** Can View

To export vulnerability data in the new interface:

1. View vulnerability data in either of the following locations:
   - By Plugin tab on the Vulnerabilities page
   - By Asset tab on the Vulnerabilities page

2. (Optional) Refine the table data. For more information, see Tenable.io Tables.

3. (Optional) Apply a saved search to the table.

4. Select the vulnerabilities you want to export:

<table>
<thead>
<tr>
<th>Export Scope</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>All vulnerabilities on all affected assets</td>
<td>In the upper-right corner of the page, click the [→ Export button. The export file is the same, regardless of whether the By Plugin or By Asset tab is active.</td>
</tr>
<tr>
<td>All vulnerabilities on an individual asset</td>
<td>To export from the By Asset tab:</td>
</tr>
<tr>
<td></td>
<td>a. Click the By Asset tab.</td>
</tr>
<tr>
<td></td>
<td>b. In an individual row of the assets table, click the [→ button.</td>
</tr>
<tr>
<td>All vulnerabilities on multiple assets</td>
<td>To export from the By Asset tab:</td>
</tr>
<tr>
<td></td>
<td>a. Click the By Asset tab.</td>
</tr>
<tr>
<td></td>
<td>b. In the assets table, select the check box next to</td>
</tr>
<tr>
<td>An individual vulnerability on all affected assets</td>
<td>To export from the <strong>By Plugin</strong> tab, click the [→ button in an individual row of the plugins table.</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>To export from the <strong>Vulnerability Details</strong> page:</strong></td>
<td></td>
</tr>
<tr>
<td>a. In the plugins table on the <strong>By Plugin</strong> tab, click an individual row.</td>
<td></td>
</tr>
<tr>
<td>The <strong>Vulnerability Details</strong> page appears.</td>
<td></td>
</tr>
<tr>
<td>b. In the upper-right corner, click the <strong>Actions</strong> button.</td>
<td></td>
</tr>
<tr>
<td>The actions menu appears.</td>
<td></td>
</tr>
<tr>
<td>c. In the actions menu, click [→ <strong>Export</strong>.</td>
<td></td>
</tr>
<tr>
<td>An individual vulnerability on an individual asset</td>
<td>To export from the <strong>By Plugin</strong> tab:</td>
</tr>
<tr>
<td>a. In the plugins table, click an individual row.</td>
<td></td>
</tr>
<tr>
<td>The <strong>Vulnerability Details</strong> page appears.</td>
<td></td>
</tr>
<tr>
<td>b. In the <strong>Output</strong> section of the <strong>Details</strong> tab, locate the box for the vulnerability you want to export.</td>
<td></td>
</tr>
<tr>
<td>c. In the upper-right corner of the plugin output box, click the [→ button.</td>
<td></td>
</tr>
<tr>
<td><strong>To export from the <strong>Asset Details</strong> page:</strong></td>
<td></td>
</tr>
<tr>
<td>a. Click the <strong>By Asset</strong> tab.</td>
<td></td>
</tr>
<tr>
<td>b. In the assets table, click an individual row.</td>
<td></td>
</tr>
<tr>
<td>The <strong>Asset Details</strong> page appears.</td>
<td></td>
</tr>
<tr>
<td>An individual vulnerability on multiple assets</td>
<td>To export from the <strong>By Plugin</strong> tab:</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>c. In an individual row of the vulnerabilities table, click the [⇒ button.</td>
<td>a. In the plugins table on the <strong>By Plugin</strong> tab, click an individual row. The <strong>Vulnerability Details</strong> page appears.</td>
</tr>
<tr>
<td></td>
<td>b. Click the <strong>Assets Affected</strong> tab.</td>
</tr>
<tr>
<td></td>
<td>c. In the assets table, select the check box for each asset you want to export. The action bar appears at the bottom of the page.</td>
</tr>
<tr>
<td></td>
<td>d. In the action bar, click the [⇒ button.</td>
</tr>
<tr>
<td>Multiple vulnerabilities on all affected assets</td>
<td>To export from the <strong>By Plugin</strong> tab:</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td></td>
<td>a. In the <strong>Output</strong> section, select the check box next to each vulnerability you want to export. The action bar appears at the bottom of the page.</td>
</tr>
<tr>
<td></td>
<td>b. In the action bar, click the [⇒ button.</td>
</tr>
<tr>
<td>Multiple vulnerabilities on an individual asset</td>
<td>To export from the <strong>By Asset</strong> tab:</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td></td>
<td>a. Click the <strong>By Asset</strong> tab.</td>
</tr>
<tr>
<td></td>
<td>b. In the assets table, click an individual row. The <strong>Asset Details</strong> page appears.</td>
</tr>
<tr>
<td></td>
<td>c. In the plugins table, select the check box next to each vulnerability you want to export. The action bar appears at the bottom of the page.</td>
</tr>
</tbody>
</table>
Multiple vulnerabilities on multiple assets

To export from the By Asset tab:

a. Click the By Asset tab.

b. Filter the assets table on the vulnerabilities you want to export.

c. In the assets table, select the check box for each asset you want to export.

The action bar appears at the bottom of the page.

d. In the action bar, click the [→] button.

e. This exports all vulnerabilities for the selected assets.

The **Exports** plane appears. This plane contains:

- A brief description of the export scope you selected under the Export label. This description specifies the number of vulnerabilities you selected for the export, whether you added additional filters to the data, and the number of affected assets you selected for the export.

  For example, **All Vulns** indicates that you selected all vulnerabilities on all affected assets, and **All Filtered Vulns for 5 Assets** indicates that you selected all vulnerabilities on multiple assets and also filtered the data.

- A list of available export formats.

5. Click the export format you want to use:

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDF - Current</td>
<td>Adobe PDF file.</td>
</tr>
<tr>
<td>PDF - Exec-</td>
<td></td>
</tr>
<tr>
<td>Format</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Executive Summary</td>
<td></td>
</tr>
<tr>
<td>HTML - Current</td>
<td>Web-based HTML file.</td>
</tr>
<tr>
<td>HTML - Executive Summary</td>
<td></td>
</tr>
<tr>
<td>Nessus</td>
<td>Nessus file. Nessus exports are the only file format that you can import into Tenable.io.</td>
</tr>
<tr>
<td>CSV</td>
<td>.csv text file.</td>
</tr>
</tbody>
</table>

If you chose this format, a list of export fields appears. You can select which fields the export includes by selecting the check box next to any field. To view only the selected fields, click **View Selected**. To view all possible fields, click **View All**.

For more information, see [CSV Export Fields](#).

**Note:** Tenable.io supports tag filters in the CSV export format only.

Tenable.io begins processing the report. Depending on the size of the exported data, Tenable.io may take several minutes to process the report.

When processing completes, Tenable.io downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

6. Access the export file via your browser's downloads directory.
## CSV Vulnerability Export Fields

Each line in the .csv file is composed of the fields described in the following table. On the **Vulnerabilities** page, you can export vulnerabilities as a .csv file.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset UUID</td>
<td>The UUID of the asset where a scan detected the vulnerability. This value is unique to Tenable.io.</td>
</tr>
<tr>
<td>CVE</td>
<td>The Common Vulnerability and Exposure (CVE) ID for the plugin that identified the vulnerability.</td>
</tr>
<tr>
<td>CVSS</td>
<td>The <strong>severity</strong> of the vulnerability.</td>
</tr>
<tr>
<td>CVSS Base Score</td>
<td>The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).</td>
</tr>
<tr>
<td>CVSS Temporal Score</td>
<td>The CVSSv2 temporal score (characteristics of a vulnerability that change over time but not among user environments).</td>
</tr>
<tr>
<td>CVSS Temporal Vector</td>
<td>CVSSv2 temporal metrics for the vulnerability.</td>
</tr>
<tr>
<td>CVSS Vector</td>
<td>Additional CVSSv2 metrics for the vulnerability.</td>
</tr>
<tr>
<td>CVSS3 Base Score</td>
<td>The CVSSv3 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).</td>
</tr>
<tr>
<td>CVSS3 Temporal Score</td>
<td>The CVSSv3 temporal score (characteristics of a vulnerability that change over time but not among user environments).</td>
</tr>
<tr>
<td>CVSS3 Temporal Vector</td>
<td>CVSSv3 temporal metrics for the vulnerability.</td>
</tr>
<tr>
<td>CVSS3 Vector</td>
<td>Additional CVSSv3 metrics for the vulnerability.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the plugin used to detect the vulnerability.</td>
</tr>
<tr>
<td>FQDN</td>
<td>The fully-qualified domain name of the host that the vulnerability was detected on.</td>
</tr>
<tr>
<td>Host</td>
<td>The hostname of the asset where a scan found the vulnerability.</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Host End</td>
<td>The UNIX timestamp for when the scan completed.</td>
</tr>
<tr>
<td>Host Start</td>
<td>The UNIX timestamp for when the scan began.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The hostname of the asset where a scan found the vulnerability.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the host where a scan found the vulnerability.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the plugin that detected the vulnerability.</td>
</tr>
<tr>
<td>NetBios</td>
<td>The NetBios name of the host where a scan found the vulnerability.</td>
</tr>
<tr>
<td>OS</td>
<td>The operating system of the host where a scan found the vulnerability.</td>
</tr>
<tr>
<td>Plugin Family</td>
<td>The plugin family of the exported vulnerabilities.</td>
</tr>
<tr>
<td>Plugin ID</td>
<td>The ID of the plugin that identified the vulnerability.</td>
</tr>
<tr>
<td>Plugin Output</td>
<td>The text output of the plugin that identified the vulnerability.</td>
</tr>
<tr>
<td>Port</td>
<td>Information about the port the scanner used to connect to the asset where the scan found the vulnerability.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol the scanner used to communicate with the asset where the scan found the vulnerability.</td>
</tr>
<tr>
<td>Risk</td>
<td>The CVSS-based risk factor associated with the plugin.</td>
</tr>
<tr>
<td>See Also</td>
<td>Links to external websites that contain helpful information about the vulnerability.</td>
</tr>
<tr>
<td>Solution</td>
<td>Remediation information for the vulnerability.</td>
</tr>
<tr>
<td>Synopsis</td>
<td>Brief description of the plugin or vulnerability.</td>
</tr>
<tr>
<td>System Type</td>
<td>Device type.</td>
</tr>
<tr>
<td>Vulnerability Priority Rating (VPR)</td>
<td>The VPR that Tenable calculates for the vulnerability. For more information, see Risk Metrics.</td>
</tr>
<tr>
<td>Vulnerability State</td>
<td>The state of the vulnerability. For more information, see Vulnerability States.</td>
</tr>
</tbody>
</table>
Vulnerability Filters

On the Vulnerabilities page, you can filter vulnerabilities using Tenable-provided filters and filters based on asset tags.

Tenable-provided Filters

Tenable.io provides the following vulnerability filters:

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset ID</td>
<td>The UUID of the asset where a scan detected the vulnerability. This value is unique to Tenable.io.</td>
</tr>
<tr>
<td>Bugtraq ID</td>
<td>The Bugtraq ID for the plugin that identified the vulnerability.</td>
</tr>
<tr>
<td>CANVAS Exploit Framework</td>
<td>Indicates whether an exploit for the vulnerability exists in the Immunity CANVAS framework.</td>
</tr>
<tr>
<td>CANVAS Package</td>
<td>The name of the CANVAS exploit pack that includes the vulnerability.</td>
</tr>
<tr>
<td>CERT Advisory ID</td>
<td>The ID of the CERT advisory related to the vulnerability.</td>
</tr>
<tr>
<td>CERT Vulnerability ID</td>
<td>The ID of the vulnerability in the CERT Vulnerability Notes Database.</td>
</tr>
<tr>
<td>Check Name</td>
<td>The description of the compliance check that detected the vulnerability.</td>
</tr>
<tr>
<td>Compliance Reference</td>
<td>The name of the reference file the scan used for the compliance check.</td>
</tr>
<tr>
<td>CORE Exploit Framework</td>
<td>Indicates whether an exploit for the vulnerability exists in the CORE Impact framework.</td>
</tr>
<tr>
<td>CPE</td>
<td>The Common Platform Enumeration (CPE) numbers for vulnerabilities that the plugin identifies.</td>
</tr>
<tr>
<td>CVE</td>
<td>The Common Vulnerability and Exposure (CVE) IDs for the vulnerabilities that the plugin identifies.</td>
</tr>
<tr>
<td><strong>CVSS Base Score</strong></td>
<td>The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>CVSS Temporal Score</strong></td>
<td>The CVSSv2 temporal score (characteristics of a vulnerability that change over time but not among user environments).</td>
</tr>
<tr>
<td><strong>CVSS Temporal Vector</strong></td>
<td>CVSSv2 temporal metrics for the vulnerability.</td>
</tr>
<tr>
<td><strong>CVSS v3.0 Base Score</strong></td>
<td>The CVSSv3 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).</td>
</tr>
<tr>
<td><strong>CVSS v3.0 Temporal Score</strong></td>
<td>The CVSSv3 temporal score (characteristics of a vulnerability that change over time but not among user environments).</td>
</tr>
<tr>
<td><strong>CVSS v3.0 Temporal Vector</strong></td>
<td>CVSSv3 temporal metrics for the vulnerability.</td>
</tr>
<tr>
<td><strong>CVSS v3.0 Vector</strong></td>
<td>Additional CVSSv3 metrics for the vulnerability.</td>
</tr>
<tr>
<td><strong>CVSS Vector</strong></td>
<td>The raw CVSSv2 metrics for the vulnerability. For more information, see CVSSv2 documentation.</td>
</tr>
<tr>
<td><strong>CWE</strong></td>
<td>The Common Weakness Enumeration (CWE) for the vulnerability.</td>
</tr>
<tr>
<td><strong>Check Name</strong></td>
<td>The description of the compliance check that detected the vulnerability.</td>
</tr>
<tr>
<td><strong>Compliance Reference</strong></td>
<td>The name of the reference file the scan used for the compliance check.</td>
</tr>
<tr>
<td><strong>Default/Known Accounts</strong></td>
<td>Indicates whether the plugin that identified the vulnerability checks for default accounts.</td>
</tr>
<tr>
<td><strong>Elliot Exploit Framework</strong></td>
<td>Indicates whether an exploit for the vulnerability exists in the D2 Elliot Web Exploitation framework.</td>
</tr>
<tr>
<td><strong>Elliot Exploit Name</strong></td>
<td>The name of the exploit for the vulnerability in the D2 Elliot Web Exploitation framework.</td>
</tr>
<tr>
<td><strong>Exploit Available</strong></td>
<td>Indicates whether a public exploit exists for the vulnerability.</td>
</tr>
<tr>
<td><strong>Exploit Database ID</strong></td>
<td>The ID of the vulnerability in the Exploit Database.</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td><strong>ExploitHub</strong></td>
<td>Indicates whether an exploit for the vulnerability exists in the ExploitHub framework.</td>
</tr>
<tr>
<td><strong>Exploitability Ease</strong></td>
<td>Description of how easy it is to exploit the vulnerability.</td>
</tr>
<tr>
<td><strong>Exploited by Malware</strong></td>
<td>Indicates whether the vulnerability is known to be exploited by malware.</td>
</tr>
<tr>
<td><strong>Exploited by Nessus</strong></td>
<td>Indicates whether Nessus exploited the vulnerability during the process of identification.</td>
</tr>
<tr>
<td><strong>ExploitHub</strong></td>
<td>Indicates whether an exploit for the vulnerability exists in the ExploitHub framework.</td>
</tr>
<tr>
<td><strong>Hostname/IP Address</strong></td>
<td>The host name of the asset where a scan found the vulnerability.</td>
</tr>
<tr>
<td><strong>Note:</strong> Ensure the search query does not end in a period.</td>
<td></td>
</tr>
<tr>
<td><strong>IAVA ID</strong></td>
<td>The ID of the information assurance vulnerability alert (IAVA) for the vulnerability.</td>
</tr>
<tr>
<td><strong>IAVB ID</strong></td>
<td>The ID of the information assurance vulnerability bulletin (IAVB) for the vulnerability.</td>
</tr>
<tr>
<td><strong>IAVM Severity</strong></td>
<td>The severity of the vulnerability in Information Assurance Vulnerability Management (IAVM).</td>
</tr>
<tr>
<td><strong>IAVT ID</strong></td>
<td>The ID of the information assurance vulnerability technical bulletin (IAVT) for the vulnerability.</td>
</tr>
<tr>
<td><strong>In the News</strong></td>
<td>Indicates whether this plugin has received media attention (for example, ShellShock, Meltdown).</td>
</tr>
<tr>
<td><strong>Malware</strong></td>
<td>Indicates whether the plugin that identified the vulnerability checks for malware.</td>
</tr>
<tr>
<td><strong>Metasploit Exploit</strong></td>
<td>Indicates whether an exploit for the vulnerability exists in the Metasploit</td>
</tr>
<tr>
<td>Framework</td>
<td>framework.</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
</tr>
<tr>
<td>Metasploit Name</td>
<td>The name of the related exploit in the Metasploit framework.</td>
</tr>
<tr>
<td>Microsoft Bulletin</td>
<td>The Microsoft security bulletin that the plugin that identified the vulnerability covers.</td>
</tr>
<tr>
<td>OSVDB ID</td>
<td>The ID of the vulnerability in the Open Sourced Vulnerability Database (OSVDB).</td>
</tr>
<tr>
<td>Patch Publication Date</td>
<td>The date on which the vendor published a patch for the vulnerability.</td>
</tr>
<tr>
<td>Plugin Description</td>
<td>The description of the Tenable plugin that identified the vulnerability.</td>
</tr>
<tr>
<td>Plugin Family</td>
<td>The family of the plugin that identified the vulnerability.</td>
</tr>
<tr>
<td>Plugin ID</td>
<td>The ID of the plugin that identified the vulnerability.</td>
</tr>
<tr>
<td>Plugin Modification Date</td>
<td>The date on which the plugin was last modified.</td>
</tr>
<tr>
<td>Plugin Name</td>
<td>The name of the plugin that identified the vulnerability.</td>
</tr>
<tr>
<td>Plugin Output</td>
<td>The text output of the Nessus scanner that identified the vulnerability.</td>
</tr>
<tr>
<td>Plugin Publication Date</td>
<td>The date on which the plugin that identified the vulnerability was published.</td>
</tr>
<tr>
<td>Plugin Type</td>
<td>The general type of plugin check (for example, local or remote).</td>
</tr>
<tr>
<td>Port</td>
<td>Information about the port the scanner used to connect to the asset where the scan detected the vulnerability.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol the scanner used to communicate with the asset where the scan detected the vulnerability.</td>
</tr>
<tr>
<td>Recast &amp; Accept</td>
<td>Indicates whether the vulnerability is affected by a recast or accept rule.</td>
</tr>
<tr>
<td>Secunia ID</td>
<td>The ID of the Secunia research advisory related to the vulnerability.</td>
</tr>
<tr>
<td>See Also</td>
<td>Links to external websites that contain helpful information about the vulnerability.</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>The vulnerability's CVSS-based severity. For more information, see <a href="#">CVSS vs. VPR</a>.</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td>A brief summary of how you can remediate the vulnerability.</td>
</tr>
<tr>
<td><strong>Synopsis</strong></td>
<td>Brief description of the plugin or vulnerability.</td>
</tr>
<tr>
<td><strong>Tag (Category: Value)</strong></td>
<td>A unique filter that searches tags (category: value) pairs. For more information, see <a href="#">tags</a>.</td>
</tr>
</tbody>
</table>

**Note:** When filtering by tag, Tenable.io displays up to 25,000 tag results. To view the full results, refine your tag filter, or [export](#) the vulnerability data.

<table>
<thead>
<tr>
<th><strong>Target Group</strong></th>
<th>A target group. For more information, see <a href="#">Target Groups</a>.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unsupported By Vendor</strong></td>
<td>Software found by this plugin is unsupported by the software's vendor (for example, Windows 95 or Firefox 3).</td>
</tr>
<tr>
<td><strong>Vulnerability First Seen</strong></td>
<td>The date when a scan first found the vulnerability on an asset.</td>
</tr>
<tr>
<td><strong>Vulnerability Last Seen</strong></td>
<td>The date when a scan last found the vulnerability on an asset.</td>
</tr>
<tr>
<td><strong>Vulnerability Priority Rating (VPR)</strong></td>
<td>The <a href="#">VPR</a> Tenable calculated for the vulnerability.</td>
</tr>
<tr>
<td><strong>Vulnerability Publication Date</strong></td>
<td>The date when the vulnerability definition was first published (for example, the date that the CVE was published).</td>
</tr>
<tr>
<td><strong>Vulnerability State</strong></td>
<td>The state of the vulnerability. For more information, see <a href="#">Vulnerability States</a>.</td>
</tr>
</tbody>
</table>

---

### Tenable.io Web Application Scanning Vulnerability Filters

<table>
<thead>
<tr>
<th><strong>Filter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application</strong></td>
<td>The number of applications affected by the vulnerability.</td>
</tr>
<tr>
<td>Count</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Bugtraq Id</td>
<td>The Bugtraq ID for the plugin that identified the vulnerability.</td>
</tr>
<tr>
<td>CPE</td>
<td>The Common Platform Enumeration (CPE) numbers for vulnerabilities that the plugin identifies.</td>
</tr>
<tr>
<td>CVE</td>
<td>The Common Vulnerability and Exposure (CVE) IDs for the vulnerabilities that the plugin identifies.</td>
</tr>
<tr>
<td>CVSS Base Score</td>
<td>The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).</td>
</tr>
<tr>
<td>CVSS v3.0 Base Score</td>
<td>The CVSSv3 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).</td>
</tr>
<tr>
<td>CVSS v3.0 Vector</td>
<td>Additional CVSSv3 metrics for the vulnerability.</td>
</tr>
<tr>
<td>CVSS Vector</td>
<td>The raw CVSSv2 metrics for the vulnerability. For more information, see CVSSv2 documentation.</td>
</tr>
<tr>
<td>CWE</td>
<td>The Common Weakness Enumeration (CWE) for the vulnerability.</td>
</tr>
<tr>
<td>First Seen</td>
<td>The date on which the first instance of the vulnerability was detected.</td>
</tr>
<tr>
<td>Host</td>
<td>The host of the URL where the vulnerability was detected.</td>
</tr>
<tr>
<td>OWASP Top 10 2010</td>
<td>The Open Web Application Security Project (OWASP) 2010 category for the vulnerability targeted by the plugin.</td>
</tr>
<tr>
<td>OWASP Top 10 2013</td>
<td>The Open Web Application Security Project (OWASP) 2013 category for the vulnerability targeted by the plugin.</td>
</tr>
<tr>
<td>OWASP Top 10 2017</td>
<td>The Open Web Application Security Project (OWASP) 2017 category for the vulnerability targeted by the plugin.</td>
</tr>
<tr>
<td>Plugin Description</td>
<td>The description of the Tenable plugin that identified the vulnerability.</td>
</tr>
<tr>
<td>Plugin Family</td>
<td>The family of the plugin that identified the vulnerability.</td>
</tr>
<tr>
<td><strong>Plugin ID</strong></td>
<td>The ID of the plugin that identified the vulnerability.</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Plugin Mod-</strong></td>
<td>The date on which the plugin was last modified.</td>
</tr>
<tr>
<td><strong>ification Date</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Plugin Name</strong></td>
<td>The name of the plugin that identified the vulnerability.</td>
</tr>
<tr>
<td><strong>Plugin Public-</strong></td>
<td>The date on which the plugin that identified the vulnerability was published.</td>
</tr>
<tr>
<td><strong>ation Date</strong></td>
<td></td>
</tr>
<tr>
<td><strong>See Also</strong></td>
<td>Links to external websites that contain helpful information about the vulnerability.</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>The CVSS score-based severity. For more information, see CVSS Scores vs. VPR in the Tenable.io Vulnerability Management User Guide.</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td>A brief summary of how you can remediate the vulnerability.</td>
</tr>
<tr>
<td><strong>WASC</strong></td>
<td>The Web Application Security Consortium (WASC) category associated with the vulnerability targeted by the plugin.</td>
</tr>
</tbody>
</table>

### Tag Filters

In Tenable.io, tags allow you to add descriptive metadata to assets that helps you group assets by business context. For more information, see [Tags](#). On both the **By Plugin** and **By Asset** tabs of the **Vulnerabilities** page, you can **filter** vulnerabilities by tags applied to the related assets.

**Note:** When using the **contains** or **does not contain** operators, use the following best practices:

- For the most accurate and complete search results, use full words in your search value.
- Do not use periods in your search value.
- Remember that when filtering **assets**, the search values are case sensitive.
- Filter by only one value per filter. For example, to filter by two different IP addresses, add two separate filters for each IP address.
- Where applicable, Tenable recommends using the **contains** or **does not contain** instead of the **is equal to** or **is not equal to** operators.
In the **Category** drop-down box for a filter, your organization's tags appear at the bottom of the list, after the Tenable-provided filters.

If you want to export vulnerabilities filtered by tag, use the .csv export format. Tag filters are not supported in other export formats.

**Note:** If you exceed the current asset query limitation of 5,000, a message appears in your interface. You should refine the query to a smaller set of asset tags.
Application Filters in WAS

On the Vulnerabilities page, on the By Applications tab, you can filter applications using Tenable-provided filters.

Tenable-provided Filters

Tenable.io Web Application Scanning provides the following application filters:

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finding Count</td>
<td>The number of Vulnerabilities detected on the application across all scans.</td>
</tr>
<tr>
<td>First Seen</td>
<td>The date on which the application was first scanned successfully.</td>
</tr>
<tr>
<td>Host</td>
<td>The host name of the asset where a scan found the vulnerability.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>The date on which the application was last scanned successfully.</td>
</tr>
<tr>
<td>Plugin ID</td>
<td>The ID of the plugin that identified the vulnerability.</td>
</tr>
<tr>
<td>Severity</td>
<td>The CVSS score-based severity. For more information, see CVSS Scores vs. VPR in the Tenable.io Vulnerability Management User Guide.</td>
</tr>
</tbody>
</table>
Vulnerability Severity Indicators

Tenable assigns all vulnerabilities a severity (Info, Low, Medium, High, or Critical) based on the vulnerability's static CVSSv2 or CVSSv3 score, depending on your configuration. For more information, see Configure Your Severity Metric.

The Tenable.io interface uses different icons for each severity category and accepted or recasted status.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Category</th>
<th>And</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟠</td>
<td>Critical</td>
<td>You have not accepted or recasted the risk.</td>
</tr>
<tr>
<td>🟠</td>
<td></td>
<td>You accepted the risk.</td>
</tr>
<tr>
<td>🟠</td>
<td></td>
<td>You recasted the severity to Critical.</td>
</tr>
<tr>
<td>🟠</td>
<td>High</td>
<td>You have not accepted or recasted the risk.</td>
</tr>
<tr>
<td>🟠</td>
<td></td>
<td>You accepted the risk.</td>
</tr>
<tr>
<td>🟠</td>
<td></td>
<td>You recasted the severity to High.</td>
</tr>
<tr>
<td>🟠</td>
<td>Medium</td>
<td>You have not accepted or recasted the risk.</td>
</tr>
<tr>
<td>🟠</td>
<td></td>
<td>You accepted the risk.</td>
</tr>
<tr>
<td>🟠</td>
<td></td>
<td>You recasted the severity to Medium.</td>
</tr>
<tr>
<td>🟠</td>
<td>Low</td>
<td>You have not accepted or recasted the risk.</td>
</tr>
<tr>
<td>🟠</td>
<td></td>
<td>You accepted the risk.</td>
</tr>
<tr>
<td>🟠</td>
<td></td>
<td>You recasted the severity to Low.</td>
</tr>
</tbody>
</table>
# Vulnerability States

Tenable assigns a vulnerability state to all vulnerabilities detected on your network. You can track and filter by vulnerability state to see the detection, resolution, and reappearance of vulnerabilities over time.

**Note:** If you filter vulnerabilities using the **Active** state, Tenable.io also returns vulnerabilities in the **New** state. For filtering purposes, **New** is a sub-category of **Active**.

<table>
<thead>
<tr>
<th>Vulnerability State</th>
<th>Visibility</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Visible in dashboards</td>
<td>The vulnerability is currently present on a host and was first detected within the last 14 days.</td>
</tr>
<tr>
<td>Active</td>
<td>Visible in dashboards</td>
<td>The vulnerability is currently present on a host and was first detected more than 14 days ago.</td>
</tr>
<tr>
<td>Fixed</td>
<td>Hidden in dashboards, but visible with filters</td>
<td>The vulnerability was present on a host, but is no longer present.</td>
</tr>
<tr>
<td>Resurfaced</td>
<td>Visible in dashboards</td>
<td>The vulnerability was previously marked as fixed on a host, but was detected again. When a vulnerability is <strong>Resurfaced</strong>, it remains in this state until:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A later scan identifies the vulnerability as remediated, at which point the vulnerability returns to a <strong>Fixed</strong> state.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The asset data ages out (by default, 90 days), at which point the vulnerability no longer appears in aggregated scan data unless it is present on another host.</td>
</tr>
</tbody>
</table>
Vulnerabilities (Classic Interface)

**Note:** This section describes the classic Tenable.io interface. For an introduction to the new interface, see Vulnerabilities.

The **Vulnerabilities** workbench provides quick insight into your organization's use of Tenable.io, your scan operations, vulnerabilities detected, plugins used, and information about your scanned assets.

The **Vulnerabilities** workbench displays two tabs:

- **Vulnerabilities By Plugin (Classic Interface)**
- **Vulnerabilities By Asset (Classic Interface)**

On these tabs, you can filter and export vulnerability data.

**Note:** The **By Plugin** tab is the Tenable.io default landing page. When clicked, the **Tenable** logo redirects to the **By Plugin** tab.
Vulnerabilities By Plugin (Classic Interface)

The **By Plugin** tab is the default landing page for Tenable.io. This tab contains charts that display vulnerabilities detected across all scanned assets based on the applied filter. To filter the **Vulnerabilities by Plugin** page, see [Filter the Vulnerabilities or Assets Workbench (Classic Interface)](#).

![Vulnerabilities by Plugin tab](image)

**Charts**

The following table contains a description of each chart on the **By Plugin** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Vulnerabilities</td>
<td>Displays the number of detected vulnerabilities, organized by severity category: <strong>CRITICAL</strong>, <strong>HIGH</strong>, <strong>MEDIUM</strong>, or <strong>LOW</strong>. For more information, see <a href="#">CVSS vs. VPR</a>. Click a tile to view a list of vulnerabilities, filtered by the severity category.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>you selected.</td>
<td></td>
</tr>
<tr>
<td><strong>Vulnerabilities Over Time</strong></td>
<td>Displays the number of vulnerabilities detected per day. Each line represents a count of the vulnerabilities in each severity category. Each data point represents all of the vulnerabilities with that severity category discovered in one day. Click the <strong>Vulnerability Trending</strong> text to view the <strong>Vulnerability Trending</strong> widget in the new interface, as described in <a href="#">Vulnerability Management Overview Dashboard</a>.</td>
</tr>
<tr>
<td><strong>Vulnerability Priority Rating (VPR)</strong></td>
<td>Displays the number of vulnerabilities present on your network that have a calculated VPR, organized by VPR range. For more information, see <a href="#">CVSS vs. VPR</a>. Click a tile to view a <strong>list of vulnerabilities</strong>, filtered by the VPR category you selected.</td>
</tr>
<tr>
<td><strong>Exploit Available</strong></td>
<td>Displays the number of detected vulnerabilities that have publicly available exploits. Click the chart to view a <strong>list of vulnerabilities</strong>, filtered to show vulnerabilities with publicly available exploits.</td>
</tr>
<tr>
<td><strong>Published Over 30 Days Ago</strong></td>
<td>Displays the number of detected vulnerabilities that were published more than 30 days ago. Click the chart to view a <strong>list of vulnerabilities</strong>, filtered to show vulnerabilities published more than 30 days ago.</td>
</tr>
<tr>
<td><strong>Discovered Using Credentials</strong></td>
<td>Displays the number of vulnerabilities that were detected using system credentialed checks. Click the chart to view a <strong>list of vulnerabilities</strong>, filtered to show vulnerabilities that were detected using system credentialed checks.</td>
</tr>
<tr>
<td><strong>Published Solutions</strong></td>
<td>Displays the number of detected vulnerabilities that have remediation</td>
</tr>
</tbody>
</table>
Plugin List

The following table contains a description of each element in the list of plugins used on the By Plugin tab. Click a row to view the plugin details, as described in Plugin Details (Classic Interface).

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count</td>
<td>Displays the number of vulnerable assets based on the discoveries made by the listed plugin. The vulnerable assets appear on the plugin's detail page.</td>
</tr>
<tr>
<td>Family</td>
<td>Displays the name of the plugin family to which the listed plugin belongs.</td>
</tr>
<tr>
<td>Name</td>
<td>Displays the name of the plugin used to detect a vulnerability. A plugin name will appear only once in the list, even if it was used to discover multiple vulnerabilities.</td>
</tr>
<tr>
<td>Severity</td>
<td>Displays a colored dot that indicates the severity level of the vulnerabilities detected by the plugin. The severity also appears on the plugin's detail page.</td>
</tr>
<tr>
<td>State</td>
<td>Displays a badge that shows the status of the vulnerability. For more information, see Vulnerability States (Classic Interface).</td>
</tr>
<tr>
<td>Total Count</td>
<td>Displays the total number of times a single plugin was used to detect a vulnerability within the selected time span.</td>
</tr>
<tr>
<td>E.g., if 10 assets are scanned and the same plugin is used to detect the same vulnerability on each asset, the Total Count number is 10.</td>
<td></td>
</tr>
<tr>
<td>Total Plugins</td>
<td>Displays the total number of individual plugins used to detect vulnerabilities within the selected time span.</td>
</tr>
<tr>
<td>E.g., if 20 assets are scanned and the same plugin is used to detect the same vulnerability on each asset, the Total Plugins number is 1.</td>
<td></td>
</tr>
<tr>
<td>Element</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>VPR</td>
<td>Displays the highest VPR calculated for any of the vulnerabilities associated with the plugin.</td>
</tr>
</tbody>
</table>
Vulnerabilities By Asset (Classic Interface)

The **By Asset** tab contains charts that display detected data about scanned assets based on the applied filter. For more information, see Filter the Vulnerabilities or Assets Workbench (Classic Interface).

The following table contains a description of each chart on the **By Asset** tab.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Displays the operating systems identified across all scanned assets within the selected time span.</td>
</tr>
</tbody>
</table>
### Name | Description
---|---
Hover over a wedge of the chart to view the percentage of assets with that operating system.
Device Types | Displays the hardware device types identified across all scanned assets within the selected time span.
Hover over a wedge of the chart to view the percentage of assets with that hardware device type.
Authentication | Displays the authentication methods used across all scans performed within the selected time span.
Hover over a wedge of the chart to view the percentage of scans performed with that authentication method.
Last Scanned | Displays the percentage of assets scanned based on recent scans within the selected time span.
Hover over a wedge of the chart to view the percentage of assets scanned.
Assets Over Time | Displays the number of assets scanned per day within the selected time span.
Each data point represents all of the assets scanned in one day.

**Note:** This table does not appear when the selected time span is All.

### Asset List

The list of assets on the **By Asset** tab displays the vulnerabilities detected on each host asset scanned. The following table contains a description of each element in the list of assets.

#### Element | Description
---|---
All Assets | Displays the total number of assets scanned within the selected time span.
<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>Displays the name of the scanned asset.</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>Displays a bar chart with asset vulnerability counts for each severity category. More information about the detected vulnerabilities is available on the asset's detail page.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>Displays the date on which the asset was last scanned.</td>
</tr>
</tbody>
</table>
Plugin Details (Classic Interface)

You can drill into the plugin details page from assets or vulnerability pages to view detailed information about the plugin, vulnerability, and assets.

On this page, you can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export drop-down box</td>
<td>Export plugin details.</td>
</tr>
<tr>
<td>Description</td>
<td>View information about the plugin, vulnerability instance, and affected assets.</td>
</tr>
<tr>
<td>Solution</td>
<td>View a brief summary of how you can remediate the vulnerability.</td>
</tr>
<tr>
<td>See Also</td>
<td>Click links to external resources related to the vulnerability.</td>
</tr>
<tr>
<td>Output</td>
<td>View the plugin output.</td>
</tr>
<tr>
<td>Plugin Details</td>
<td>View details about the plugin.</td>
</tr>
<tr>
<td>Discovery</td>
<td>View details about when the vulnerability was discovered and last seen on your network.</td>
</tr>
<tr>
<td>Vulnerability Priority Rating (VPR) Key Drivers</td>
<td>View the key drivers Tenable used to calculate the vulnerability VPR. For more information about VPR key drivers, see CVSS vs. VPR.</td>
</tr>
<tr>
<td>Risk Information</td>
<td>View metrics (e.g., CVSS score) about the risk associated with the vulnerability.</td>
</tr>
<tr>
<td>Vulnerability Information</td>
<td>View details about the vulnerability’s exploitability.</td>
</tr>
<tr>
<td>Reference Information</td>
<td>View related links to the CVE, BID, MSFT, CERT, and other industry materials about the vulnerability.</td>
</tr>
</tbody>
</table>
Vulnerability States (Classic Interface)

Tenable assigns a vulnerability state to all vulnerabilities detected on your network. You can track and filter by vulnerability state to see the detection, resolution, and reappearance of vulnerabilities over time. States appear as text badges in the tables that appear on the Vulnerabilities workbench.

<table>
<thead>
<tr>
<th>Vulnerability State</th>
<th>Visibility</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Visible in work-benches</td>
<td>The vulnerability is currently present on a host and was first detected within the last 14 days.</td>
</tr>
<tr>
<td>Active</td>
<td>Visible in work-benches</td>
<td>The vulnerability is currently present on a host and was first detected more than 14 days ago.</td>
</tr>
<tr>
<td>Fixed</td>
<td>Hidden in work-benches, but visible with filters</td>
<td>The vulnerability was present on a host, but is no longer present.</td>
</tr>
<tr>
<td>Resurfaced</td>
<td>Visible in work-benches</td>
<td>The vulnerability was previously marked as fixed on a host, but was detected again.</td>
</tr>
</tbody>
</table>
Solutions

Tenable provides recommended solutions for all vulnerabilities on your network. You can sort recommended solutions by VPR to identify your highest priority solutions, then drill into the solution details to understand the steps to address the vulnerability on your network.

**Note:** You cannot view solution details without a Lumin license. For more information, see [Lumin](#).

For more information, see:

- [View Solutions](#)
- [Export Solutions](#)
- [View Solution Details](#)
View Solutions

**Required Additional License:** Tenable Lumin

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

Tenable provides recommended solutions for all vulnerabilities on your network. You can sort recommended solutions by [Vulnerability Priority Rating (VPR)](#) to identify your highest priority solutions, then drill into the solution details to understand the steps to address the vulnerability on your network.

Addressing a vulnerability instance lowers your [CES](#) and [AES](#) metrics.

**Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

To view solutions in the new interface:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation plane, in the Vulnerability Management section, click Solutions.

   The Solutions page appears.

   **Note:** All Lumin data reflects all assets within the organization's Tenable.io instance.

On this page, you can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filters</td>
<td>Filter the data displayed in the table.</td>
</tr>
<tr>
<td>Saved Searches</td>
<td>• Load or edit an existing saved search.</td>
</tr>
<tr>
<td></td>
<td>• Save a new saved search.</td>
</tr>
<tr>
<td>Export</td>
<td>Export a solution as a .csv file.</td>
</tr>
<tr>
<td>Solutions table</td>
<td>• View information about each solution.</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• <strong>Solution</strong> — A description for the solution.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Assets Affected</strong> — The total number of assets affected by the vulnerabilities addressed by the solution.</td>
</tr>
<tr>
<td></td>
<td>• <strong>CVE Count</strong> — The CVEs included in the solution.</td>
</tr>
<tr>
<td></td>
<td>• <strong>VPR</strong> — The highest <a href="#">VPR</a> for the vulnerabilities addressed by the solution.</td>
</tr>
<tr>
<td></td>
<td>• <strong>CVSS</strong> — The highest CVSSv2 score (or CVSSv3 score, when available) for the vulnerabilities addressed by the solution.</td>
</tr>
<tr>
<td></td>
<td>• To view details for a solution, click a solution row. The Solution Details page appears. For more information, see Solution Details.</td>
</tr>
<tr>
<td></td>
<td>• To sort, increase or decrease the number of rows per page, or navigate to another page of the table, see <a href="#">Tenable.io Tables</a>.</td>
</tr>
</tbody>
</table>
Export Solutions

**Required Additional License:** Tenable Lumin

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

In the new interface, the export feature allows you to export solution data .csv file format.

To export solutions as a .csv file:

1. In the upper-left corner, click the button.
   
   The left navigation plane appears.

2. In the left navigation plane, in the Vulnerability Management section, click Solutions.
   
   The Solutions page appears.

3. In the upper-right hand corner, click [Export].
   
   The Export plane appears.

4. View the selected format for the export: CSV.

5. Click the check box next to the Data option you want included in the export file.

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solutions</td>
<td>Includes solutions data.</td>
</tr>
<tr>
<td>Details</td>
<td>Includes solutions data and data for assets affected where Tenable recommends the solutions.</td>
</tr>
</tbody>
</table>

6. Click Export.

   Tenable.io begins processing the report. Depending on the size of the exported data, Tenable.io may take several minutes to process the report.

   When processing completes, Tenable.io downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

7. Access the export file via your browser’s downloads directory.
View Solution Details

**Required Additional License:** Tenable Lumin

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can use this page to view details for a solution, including asset and vulnerability information.

To view solution details in the new interface:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Vulnerability Management** section, click **Solutions**.

   The **Solutions** page appears.

3. Click a solution row.

   The **Solution Details** page appears.

On this page, you can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary panel</td>
<td>View summary statistics for the recommended solution.</td>
</tr>
<tr>
<td>Metrics summary</td>
<td>- <strong>Assets Affected</strong> – The total number of assets affected by the vulnerabilities addressed by the solution.</td>
</tr>
<tr>
<td></td>
<td>- <strong>CVE Count</strong> – The total number of CVEs included in the solution.</td>
</tr>
<tr>
<td></td>
<td>- <strong>CVE Instances</strong> – The total number of vulnerabilities addressed by the solution.</td>
</tr>
<tr>
<td></td>
<td>- <strong>VPR</strong> – The highest <strong>VPR</strong> for a vulnerability included in the solution.</td>
</tr>
</tbody>
</table>

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
<table>
<thead>
<tr>
<th><strong>Vulnerabilities Included (#) table</strong></th>
<th>View all vulnerabilities addressed by the solution.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>Identifier</strong> – The vulnerability identifier: the CVE (if available), the TVI, or the plugin ID.</td>
</tr>
<tr>
<td></td>
<td>• <strong>VPR</strong> – The VPR for the vulnerability.</td>
</tr>
<tr>
<td></td>
<td>• <strong>CVSS</strong> – The CVSSv2 score (or CVSSv3 score, when available) for the vulnerability.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Assets Affected</strong> – The total number of assets affected by the vulnerability.</td>
</tr>
<tr>
<td></td>
<td>• To view details about a vulnerability, click a vulnerability row. The vulnerability details plane appears. On this plane, you can:</td>
</tr>
<tr>
<td></td>
<td>• View a summary of the vulnerability.</td>
</tr>
<tr>
<td></td>
<td>• View information about the key drivers Tenable used to calculate the VPR for this vulnerability.</td>
</tr>
<tr>
<td></td>
<td>• View a graph that shows the VPR adjustments over the past 30 days, compared to the static CVSSv2 score (or CVSSv3 score, when available).</td>
</tr>
<tr>
<td></td>
<td>• View additional information about the vulnerability, including the TVI.</td>
</tr>
<tr>
<td></td>
<td>• To navigate to another page of the table, see Tenable.io Tables.</td>
</tr>
</tbody>
</table>

| **Assets Affected tab** | View the ACR severity tiles, which summarize the number of |
| ACR tiles | |
affected assets in the **Low, Medium, High**, or **Critical**, or **Unclassified** ACR category.

| **Assets Affected table** | • View asset information.  
  • **Asset** – The asset identifier. Tenable.io assigns this identifier based on the presence of certain asset attributes in the following order: Agent Name (if agent-scanned) NetBIOS Name FQDN IPv6 address IPv4 address. For example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the Asset Name.  
  • **IP** – The asset's IP address.  
  • **ACR** – The asset's ACR.  
  • **CVE Count** – The total number of CVEs on the asset.  
  • **OS** – The asset's operating system.  
  • **Detection Source** – The scanner type that first scanned the asset.  
  • To view details for an asset, click an asset row.  
  The **Asset Details** page appears. For more information, see **Asset Details**.  
  • To filter the assets displayed in the table, see **Filter a Table**.  
  Tenable.io refreshes the table.  
  • To sort, increase or decrease the number of rows per page, or navigate to another page of the table, see **Tenable.io Tables**. |
Dashboards

Note: This section describes the new interface. For information about the classic interface, see Dashboards and Workbenches (Classic Interface). For information about navigating the new interface, see Navigate Tenable.io (New Interface).

To access your dashboards:

1. Do one of the following:
   - On any Tenable-provided dashboard page, click the ⬇️ Dashboards button.
   - On any other page:
     a. In the upper-left corner, click the ▶️ button.
        The left navigation plane appears.
     b. In the left navigation plane, click Dashboards.

   The Dashboards page appears. The page contains tiles that represent:
   - Tenable-provided dashboards.
     Note: Depending on your license, additional dashboards are included. For example, the Lumin dashboard.
   - Dashboards you have created. To create a template-based or custom dashboard with Tenable-provided or custom widgets, see Create a Dashboard.
   - Dashboards that other users have shared with you. Click the Shared with Me tab to only view dashboards that have been shared with you.
     Note: PCI Quarterly External scan data is intentionally excluded from dashboards, reports, and workbenches. This is due to the scan's paranoid nature, which may lead to false positives that would otherwise not be detected. For more information, see PCI ASV Scanning Overview.

2. In the upper-right corner of the page, use the sorting drop-down to manage the order in which dashboards appear on the Dashboards page.

For more information, see:
Vulnerability Management Overview Dashboard

**Note:** This section describes the new interface. For more information, see [Navigate the New Tenable.io Interface](#).

This Tenable-provided dashboard visualizes actionable insights for your vulnerability management program. Tenable.io updates dashboard data every time you run a scan.

**Note:** There may be a delay between when a scan completes and when the dashboard data updates while Tenable.io indexes the data.

You can roll over individual items to reveal additional information or click on items to drill down into details behind the data.

**Tip:** All charts on the Vulnerability Management Overview display New, Active, and Resurfaced vulnerability data. However, the counts or data displayed on each chart may differ for other reasons. For example, the Vulnerability Priority Rating (VPR) widget organizes vulnerabilities by VPR category, but the Vulnerability Trending widget graphs vulnerabilities by CVSS-based severity category. For more information about how severity and VPR metrics compare, see [CVSS vs. VPR](#).

In the Vulnerability Management Overview, you can interact with the following widgets:

<table>
<thead>
<tr>
<th>Widget</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Exposure News Feed</td>
<td>This widget highlights the most recent Tenable blog posts related to Cyber Exposure incidents.</td>
</tr>
<tr>
<td></td>
<td>- Click on a tile to navigate to the Tenable blog post.</td>
</tr>
<tr>
<td></td>
<td>- Click the ▼ or ▲ button to collapse or expand the feed.</td>
</tr>
<tr>
<td></td>
<td>- Click the ◀ or ▶ button to scroll through the tiles.</td>
</tr>
<tr>
<td>Statistics</td>
<td>This widget summarizes the highest severity vulnerabilities on for your network during the last 30 days.</td>
</tr>
<tr>
<td></td>
<td>- View a count of your total vulnerabilities and counts for the highest severity vulnerabilities (Critical and High) during the past 30 days.</td>
</tr>
<tr>
<td></td>
<td>- To view a list of vulnerabilities, click one of the counts.</td>
</tr>
</tbody>
</table>
The **Vulnerabilities** page appears, filtered by a severity if you selected the **Critical** or **High** count. For more information, see [View Vulnerabilities by Plugin](#).

- View a count of your total licensed assets, your assets discovered during the last 7 days, and your assets discovered during the last and 30 days.

If necessary, onboard your newly discovered assets.

- To view a list of assets, click one of the counts.

The **Assets** page appears, filtered by a time range if you selected the **7 days** or **30 days** count. For more information, see [View Asset Details](#).

- View a count of your scans run during the last 90 days and the percentage that succeeded and failed.

To investigate your failed scans, review your scans with the **status** **Aborted** or **Canceled**. For more information, see [View Scans](#).

- To export the data in the widget, click the ••• button and select a format.

### MS Exchange ProxyLogon/Hafnium Vulnerability

This widget summarizes the vulnerable and potentially compromised assets associated with the ProxyLogon/Hafnium exploit and other Microsoft Exchange Server vulnerabilities related to CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065. For more information, see [Finding ProxyLogon and related Microsoft Exchange Vulnerabilities](#).

- To view a list of vulnerable assets, click the **Vulnerable Assets** cell.

The **Vulnerabilities** page appears, filtered by asset, severity, and plugins indicating vulnerable assets associated with this exploit. For more information, see [View Vul-](#)
To view a list of potentially compromised assets, click the **Potentially Compromised** cell. The **Vulnerabilities** page appears, filtered by asset, severity, and plugins indicating potentially compromised assets associated with this exploit. For more information, see **View Vulnerabilities by Asset**.

- To export the data in the widget, click the ••• button and select a format.

### Asset Coverage

This widget summarizes how thoroughly your scans assessed the assets in your environment during the past 90 days.

- **Authenticated Scans** — The percentage of licensed assets scanned with authentication.

- **Unauthenticated Scans** — The percentage of licensed assets scanned without authentication.

For more information about authenticated and unauthenticated assessment scans, see [Discovery Scans vs. Assessment Scans](#).

To export the data in the widget, click the ••• button and select a format.

### Vulnerability Priority Rating (VPR)

This widget summarizes the number of vulnerabilities on your network, organized by VPR. For more information, see **CVSS vs. VPR**.

- To view a list of vulnerabilities filtered by a VPR range, click one of the tiles.

The **Vulnerabilities** page appears, filtered by the range you selected. For more information, see **View Vulnerabilities by Plugin**.
<table>
<thead>
<tr>
<th>Widget Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLA Progress: Vulnerability Age</td>
<td>This widget visualizes vulnerability counts by severity and by compliance with your Service Level Agreements (SLAs). To modify how Tenable.io calculates SLA severity, see Configure Your SLA Settings.</td>
</tr>
<tr>
<td>Vulnerability Trending</td>
<td>This widget displays the cumulative number of Critical, High, Medium, and Low severity vulnerabilities on your network over time. For more information, see CVSS vs. VPR.</td>
</tr>
<tr>
<td>Critical and High Exploit-</td>
<td>This widget summarizes the number of Critical and High sever-</td>
</tr>
</tbody>
</table>
**Vulnerabilities**

- To view the counts of your vulnerabilities by decreasing priority, view the categories and counts from left to right.

- To view a list of vulnerabilities, click one of the bars on the graph.

The **Vulnerabilities** page appears, filtered by **Critical** and **High** severity and the exploitability characteristic you selected. For more information, see [View Vulnerabilities by Plugin](#).

- To export the data in the widget, click the ••• button and select a format.

**Future Threats: Not Yet Exploitable Vulnerabilities**

This widget summarizes the vulnerabilities that are not yet exploitable, determined by their **Exploit Code Maturity** and **Vulnerability Publication Date**.

- To view the counts of your vulnerabilities by decreasing priority, view the categories and counts from upper-left to lower-right. Tenable recommends addressing vulnerabilities with proof-of-concept before those with no known exploit.

- To export the data in the widget, click the ••• button and select a format.

**Vulnerability Age**

This widget summarizes the age of your vulnerabilities (by **Vulnerability First Seen** date), organized by severity, to help you manage your SLAs. For more information about severity, see [CVSS vs. VPR](#).

- To view a list of vulnerabilities, click one of the vulnerability
The **Vulnerabilities** page appears, filtered by the **Vulnerability First Seen** date and severity you selected. For more information, see [View Vulnerabilities by Plugin](https://tenable.com/solutions).

- To export the data in the widget, click the ••• button and select a format.
WAS Dashboard

The default **Web Applications Scanning** dashboard displays data Tenable.io Web Application Scanning collects.

You can export the [Tenable.io Web Application Scanning dashboard](https://tenable.io) landing page, or export [individual widgets](#) on the page.

**Note:** WAS widgets do not support tags at this time.

Statistics

The table below describes the widgets displayed in the Statistics section of the **Web Applications Scanning** dashboard. You can view details about the data in a widget by clicking the widget.

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerabilities</td>
<td>Number of vulnerabilities Tenable.io Web Application Scanning has discovered in the last 90 days. The vulnerabilities are categorized by severity (Critical, High, Medium, Low, and Info). For information about vulnerability ratings and the severity metrics Tenable uses to analyze risk, see <a href="https://tenable.io">Severity vs. VPR in the Tenable.io Vulnerability Management User Guide</a>.</td>
</tr>
<tr>
<td>Applications</td>
<td>Number of applications scanned over time.</td>
</tr>
<tr>
<td>Scans (Last 90D)</td>
<td>Number of scans Tenable.io Web Application Scanning attempted in the last 90 days. The scans are categorized as percentages of successful or aborted scans.</td>
</tr>
</tbody>
</table>

**OWASP Top 10**

This chart displays the vulnerabilities discovered by Tenable.io Web Application Scanning that appear in the latest Open Web Application Security Project (OWASP) Top 10 Most Critical Web Application Security Risks document.
CS Dashboard

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

The **Container Security** dashboard acts as landing page for Tenable.io Container Security. This dashboard contains widgets that display high-level information about your containers, images and image repositories, and policies. Click a widget on the dashboard to view details about the item type or to import data items (e.g., images) into Tenable.io Container Security.

**Note:** For information about how Tenable.io Container Security evaluates risks for your assets, see [Risk Metrics in CS](#).

From the **Container Security** dashboard you can:

- [View Container Details](#)
- [Configure CS Connectors to Import and Scan Images](#)
- [View Scan Results for Container Images](#)
- [Manage CS Image Repositories](#)
- [Delete an Image in CS](#)
- [Manage CS Policies](#)
- [View CS Data Usage](#)

**Note:** Tenable.io Container Security uses the new interface. For more information about navigating the new interface, see:

- [Filter a Table in the New Tenable.io Interface](#)
- [Search a Table in the New Tenable.io Interface](#)
- [Log Out of the New Tenable.io Interface](#)
Configure CS Connectors to Import and Scan Images

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Connectors act as links to local or third-party registries. You can use connectors to access these registries and then import image data from them to Tenable.io Container Security.

To import and analyze container images, you must configure a connector to a registry or, in certain cases, to the registry’s own connector.

After you configure your connectors, you can view and manage your connectors from the Settings page in Tenable.io. For more information about connectors, see Connectors in the Tenable.io Vulnerability Management User Guide.

The amount of time Tenable.io Container Security takes to scan the images in your registry and display the results depends on the size and number of images you scan.

**Note:** If you use a connector to import and scan your images, Tenable.io Container Security may take up to several hours to display your images on the dashboard.

If your images do not appear on the dashboard within 24 hours of when you begin the import, contact Tenable Support.

### Tenable.io Container Security Connectors

**Note:** Tenable.io Container Security does not support connector configurations for Azure Container Registries (ACR). To import images from an ACR registry, use the Tenable.io CS Scanner.

Tenable.io Container Security supports image imports via the following connectors.

<table>
<thead>
<tr>
<th>Connector</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable.io Container Security Scanner</td>
<td>Command line operated, on-premises scanning tool that allows you to scan images without importing them into Tenable.io Container Security. To configure the Tenable.io Container Security Scanner, see Tenable.io CS Scanner.</td>
</tr>
<tr>
<td>Amazon Web Service Connector</td>
<td>Connector for assets hosted in an AWS Elastic Container Registry. To</td>
</tr>
<tr>
<td>Registry Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>vice (AWS) Elastic Container Registry (ECR)</td>
<td>configure an AWS ECR connector and import assets, see <a href="#">Configure an AWS ECR Connector to Import Images in CS</a>.</td>
</tr>
<tr>
<td>Docker</td>
<td>Connector for assets hosted in a Docker-compatible registry. To configure a connector for a Docker EE registry, see <a href="#">Configure a Local Connector to Import Images in CS</a>.</td>
</tr>
<tr>
<td>Docker EE</td>
<td>Connector for assets hosted in a Docker Enterprise Edition (EE) registry. To configure a connector for a Docker EE registry, see <a href="#">Configure a Local Connector to Import Images in CS</a>.</td>
</tr>
<tr>
<td>JFrog Artifactory</td>
<td>Connector for assets hosted in a JFrog Artifactory registry. To configure a connector for a JFrog Artifactory registry, see <a href="#">Configure a Local Connector to Import Images in CS</a>.</td>
</tr>
</tbody>
</table>
Configure an AWS ECR Connector to Import Images in CS

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable.io Container Security

**Required User Role:** Administrator

To import and analyze images hosted in an Amazon Web Service (AWS) Elastic Container Registry (ECR), you must configure your AWS ECR connector. Tenable.io Container Security then imports the images from your registry and scans the images for vulnerabilities.

The amount of time Tenable.io Container Security takes to scan the images in your registry and display the results depends on the size and number of images you scan.

**Note:** If you use a connector to import and scan your images, Tenable.io Container Security may take up to several hours to display your images on the dashboard.

If your images do not appear on the dashboard within 24 hours of when you begin the import, contact Tenable Support.

Before you begin:

- Activate your account and log in to Tenable.io Container Security, as described in [Log in to CS via the Docker CLI](#).
- Confirm the images you want to import are stored in your organization's container registry.

To configure a connector to an AWS Elastic Container Registry:

1. In the **Connectors** section of the **Container Security** dashboard, click **Create**.

   The **Select a Connector** plane appears.

2. In the **Container Security** section, click **AWS Elastic Container Registry**.

3. In the **URL** box, type the fully-qualified domain name of your ECR deployment (e.g., 579133718396.dkr.ecr.us-east-2.amazonaws.com).

4. In the **User Name** box, type **AWS**.

---

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable,Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
5. In the **Password** box, type the base 64-encoded password used in the `docker login` command, which is generated by AWS CLI.

**Tip:** If your ECR is in the us-east-2 region, you can run the `aws ecr get-login --region us-east-2` command to get the `docker login` command.

6. Do one of the following:

- To save the connector, click **Save**.

  **Note:** If you click **Save**, Tenable.io Container Security saves your configured connector but does not import your assets. To launch a manual import for the connector, see [Launch a Connector Import Manually](#).

- To save the connector and import your assets from the registry, click **Save & Import**.

  **Note:** When you import container images to scan, Tenable.io Container Security may abort the scan if the scan has been running for 60 minutes. If this happen, **Scan Failed** appears on the **Images** page in the **Vulnerabilities** and **Malware** columns for the aborted images.

  If Tenable.io Container Security aborts your scan, try simplifying your images before you import them, as described in the *Docker Documentation*. Alternatively, you can use the [Tenable.io CS Scanner](#) to scan your images without importing them to Tenable.io Container Security.

  If Tenable.io Container Security still aborts your scan, contact Tenable Support.

7. (Optional) Click **Back** to configure another connector.

**What to do next:**

- View the results of your scan, as described in [View Scan Results for Container Images](#).
Configure a Local Connector to Import Images in CS

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable.io Container Security

**Required User Role:** Administrator

To import and analyze images hosted in a local registry, you must configure your registry's connector. Tenable.io Container Security then imports the images from your registry and scans the images for vulnerabilities.

The amount of time Tenable.io Container Security takes to scan the images in your registry and display the results depends on the size and number of images you scan.

**Note:** If you use a connector to import and scan your images, Tenable.io Container Security may take up to several hours to display your images on the dashboard.

If your images do not appear on the dashboard within 24 hours of when you begin the import, contact Tenable Support.

Before you begin:

- Activate your account and log in to the web portal, as described in [Log in to CS via the Docker CLI](#).
- Confirm the images you want to import are stored in your organization’s container registry.

To configure a connector to a local container registry:

1. In the **Connectors** section of the **Container Security** dashboard, click **Create**.

   The **Select a Connector** plane appears.

2. In the **Container Security** section, click the name of the type of container registry you want to use. Alternatively, type the name of the registry in the search box.

   **Note:** If you want to connect to a registry that is not listed, contact Tenable Support and let them know that you want your container registry to be officially supported. If your registry is not listed but is Docker-
3. In the **URL** box, type your registry's URL.

4. In the **Port** box, type your registry's port ID.

5. In the **Username** box, type your username.

6. In the **Password** box, type your password.

7. Use the **Schedule Import** toggle to enable or disable scheduled imports.

   **Note:** By default, Tenable.io Container Security requests new and updated asset records every 12 hours.

   If enabled:

   - In the Import text box, type the frequency with which Tenable.io Container Security sends data requests to the registry.
   - In the drop-down box, select **Minutes**, **Hours**, or **Days**.

8. Do one of the following:

   - To save the connector, click **Save**.

     **Note:** If you click **Save**, Tenable.io Container Security saves your configured connector but does not import your assets. To launch a manual import for the connector, see **Launch a Connector Import Manually** in the **Tenable.io Vulnerability Management User Guide**.

   - To save the connector and import your assets from the registry, click **Save & Import**.

     **Note:** When you import container images to scan, Tenable.io Container Security may abort the scan if the scan has been running for 60 minutes. If this happen, **Scan Failed** appears on the **Images** page in the **Vulnerabilities** and **Malware** columns for the aborted images.

     If Tenable.io Container Security aborts your scan, try simplifying your images before you import them, as described in the **Docker Documentation**. Alternatively, you can use the **Tenable.io CS Scanner** to scan your images without importing them to Ten-
able.io Container Security.

If Tenable.io Container Security still aborts your scan, contact Tenable Support.

9. (Optional) Click **Back** to configure another connector.

What to do next:

- View the results of your scan, as described in [View Scan Results for Container Images](#).
The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable.io Container Security

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

A container is a running instance of an image. You create containers from an image each time you run the image on your application. You can create multiple containers from a single image, and you can make changes to those containers without affecting the image from which you created them.

After you perform a credentialed Nessus scan on your system, Tenable.io Container Security uses the scan results to identify images and containers and analyze each container for risk.

Tenable.io Container Security then displays the containers by scan status and risk level in the Identified Containers widget on the Container Security dashboard based on the results of the most recent scan.

**Note:** Tenable.io Container Security identifies and analyzes only the images and containers found via credentialed Nessus scans.

**Note:** Tenable.io Container Security imports and rescans your images at regular intervals, beginning when you first import and scan the images.

Before you begin:

- If Tenable.io Container Security has not yet scanned the source image used to create the container you want to analyze, use one of the following methods to import the image for scanning:
  - [Push](https://example.com) an individual image to Tenable.io Container Security.
  - [Configure CS Connectors to Import and Scan Images](https://example.com) stored in your organization's local registry.
- Use the Tenable.io CS Scanner to scan your images directly from your organization’s local registry or your machine.

- **Run** a Nessus scan on the network where your containers run, selecting the Basic Network Scan template and providing your network authentication credentials. For more information about Nessus scan templates, see Scan and Policy Templates in the Nessus User Guide.

  **Note:** Tenable.io Container Security imports data from Nessus to determine if there have ever been any changes made to files on the container. If Nessus detects file changes, Tenable recommends that you check your images and repositories and confirm that no one has accessed them without authorization.

  **Tip:** Alternatively, you can run a Nessus Agent scan on the network where the container runs. For more information, see the Nessus Agent User Guide.

To view container details:

1. In the Container Security dashboard, find the Identified Containers widget. This widget categorizes your containers by risk and scan status.

   **Note:** For information about how Tenable.io Container Security calculates container risk, see Container Risk.

2. Click the Identified Containers widget.

   The Identified Containers page appears. The identified containers table lists all the containers created from images scanned by Tenable.io Container Security.

3. In the identified containers table, you can:
   
   - **Filter** the identified containers table.
   - **Search** the identified containers table.
   - View the summary for your identified containers in the identified containers table.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Container ID</td>
<td>The ID that the software your container runs on assigned to the container.</td>
</tr>
<tr>
<td>Repository/Image:Tag</td>
<td>The repository name, image name, and image tag</td>
</tr>
<tr>
<td><strong>Risk Score</strong></td>
<td>The risk score on a scale of 1-10.</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td><strong>Scan Status</strong></td>
<td>Indicates whether Tenable.io Container Security has scanned the container's source image.</td>
</tr>
<tr>
<td></td>
<td>- ✅ – Tenable.io Container Security has scanned the source image.</td>
</tr>
<tr>
<td></td>
<td>- ⚠️ – Tenable.io Container Security has never scanned the source image.</td>
</tr>
<tr>
<td><strong>File Changed</strong></td>
<td>Indicates whether the Nessus scan detected any changes to container files.</td>
</tr>
<tr>
<td></td>
<td>- ✅ – Nessus did not detect file changes during its scan.</td>
</tr>
<tr>
<td></td>
<td>- ⚠️ – Nessus detected file changes during its scan.</td>
</tr>
<tr>
<td><strong>Vulnerabilities</strong></td>
<td>The number of vulnerabilities detected in the container.</td>
</tr>
</tbody>
</table>

**Note:** When you initiate an image import, Tenable.io Container Security immediately queues the image to be scanned. However, Tenable.io Container Security does not always complete the scan immediately. To prevent undetected vulnerabilities, Tenable recommends that you confirm any images marked as not scanned are imported for scanning. For information about how to import and scan images, see [Get Started with CS](#).
<table>
<thead>
<tr>
<th>Malware</th>
<th>The number of malware items detected in the container.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host IP</td>
<td>The IP address for the server where the container runs.</td>
</tr>
</tbody>
</table>

- View details for a specific container.
  
  a. In the identified containers table, click the row for the container you want to view. The identified containers details page appears.
  
  b. On the identified containers details page, you can:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerabilities</strong></td>
<td>• View details for each vulnerability identified in the image your identified container links to:</td>
</tr>
<tr>
<td></td>
<td>• In the <strong>Severity</strong> column, view the severity rating Tenable.io Container Security assigned the image.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: For information about how Tenable.io Container Security determines image risk, see <strong>Image Risk</strong>.</td>
</tr>
<tr>
<td></td>
<td>• In the <strong>Exposure ID</strong> column, view the vulnerability's ID.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The authority that identifies a given vulnerability determines the vulnerability’s ID format.</td>
</tr>
<tr>
<td></td>
<td>• In the <strong>Risk Score</strong> column, view the CVSSv2 score.</td>
</tr>
<tr>
<td></td>
<td>• In the <strong>Release Date</strong> column, view the date when the software on which the container runs released the vulnerability.</td>
</tr>
<tr>
<td>Malware</td>
<td>Images</td>
</tr>
<tr>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td>• Click a row in the vulnerabilities table. The vulnerability details plane appears, containing details and remediation recommendations for the vulnerability.</td>
<td></td>
</tr>
<tr>
<td>• View details about malware detected in the identified container:</td>
<td>• View details about the image your container links to.</td>
</tr>
<tr>
<td>• In the <strong>Infected File</strong> column, view the name of each infected file as it appears on the container.</td>
<td>• In the <strong>Image ID</strong> column, view the image ID.</td>
</tr>
<tr>
<td>• In the <strong>Risk Score</strong> column, view the CVSSv2 score for each infected file.</td>
<td>Note: The image ID automatically generates when the software that hosts your image (e.g., Docker) creates the image.</td>
</tr>
<tr>
<td></td>
<td>• In the <strong>Repository</strong> column, view the local repository where the image resides.</td>
</tr>
<tr>
<td></td>
<td>• In the <strong>Image Name</strong> column, view the image name as it appears in the repository.</td>
</tr>
<tr>
<td></td>
<td>• In the <strong>Tag</strong> column, view the tag associated with the image (e.g., latest).</td>
</tr>
<tr>
<td></td>
<td>• Click a row in the image table. The details page appears for the image your identified container links to. For information about the</td>
</tr>
<tr>
<td>Package Inventory</td>
<td>View details about the package in the image your identified container links to, including the package name, version, license, and type.</td>
</tr>
</tbody>
</table>
View Scan Results for Container Images

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Required Additional License: Tenable.io Container Security

Required Tenable.io Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

After Tenable.io Container Security scans your container images, you can view the detailed scan results on the Tenable.io Container Security dashboard.

Before you begin:

- Scan the container image you want to analyze using any of the following processes:
  - Push an individual image to Tenable.io Container Security.
  - Configure your connectors to import and scan images stored in your organization's local registry.
  - Use the Tenable.io CS Scanner to scan your images directly from your organization's local registry or your machine.

To view scan results for container images:

1. In the Statistics section of the Container Security dashboard, click the Images widget. The Images page appears.

2. In the images table, you can:
   - Filter the images table.
   - Search the images table.
   - View details for the image:
a. In the images table, click an image row.

The **Image Details** page appears.

b. On the **Image Details** page, you can:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerabilities</strong></td>
<td>• View vulnerability details for each vulnerability identified in the image:</td>
</tr>
<tr>
<td></td>
<td>• In the <strong>Severity</strong> column, view the severity rating Tenable.io Container Security assigned the image.</td>
</tr>
<tr>
<td></td>
<td>• In the <strong>Vulnerability</strong> column, view the vulnerability ID.</td>
</tr>
<tr>
<td></td>
<td>• In the <strong>Risk Score</strong> column, view the CVSSv2 score.</td>
</tr>
<tr>
<td></td>
<td>• In the <strong>Release Date</strong> column, view the date when the software on which the image is hosted released the vulnerability.</td>
</tr>
<tr>
<td></td>
<td>• Click a row in the vulnerabilities table.</td>
</tr>
<tr>
<td></td>
<td>A vulnerability details plane appears, containing details and remediation recommendations for the vulnerability.</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Malware</td>
<td>View details about malware identified in the image, including a list of infected files, the file types, and the MD5 and SHA256 digests of the file.</td>
</tr>
<tr>
<td>Package Inventory</td>
<td>View details about the package in the image your identified container links to, including the package name, version, license, and type.</td>
</tr>
<tr>
<td>Layer Digest</td>
<td>View the digest IDs for each layer in the image.</td>
</tr>
</tbody>
</table>
| Identified Containers | • In the **Container ID** column, view the ID that the software your container runs on assigned to each container.  
                        • In the **Hostname** column, view the name of the network on which each container runs.  
                        • In the **Host IP** column, view the IP address for the network on which each container runs.  
                        • In the **Start Date** column, view the date when the container most recently started running.  
                        **Note:** Not all networks have a hostname; some only have an IP address. |

---

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
Manage CS Image Repositories

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable.io Container Security

You automatically create an image repository when you push an image to the registry.

To manage image repositories in Tenable.io Container Security:

1. In the **Statistics** section of the **Container Security** dashboard, click the **Repositories** widget.

   The **Repositories** page appears, displaying an overview description of the repository.

2. In the repositories table, you can:

   - **Search the table.**

     **Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

     a. In the text box, type your search term or terms.

     b. Click the button.

     Tenable.io filters the table by your search criteria.

     **Tip:** In the top navigation bar, click a link in the breadcrumb trail to return to a previous page.

   - **View details for an image in the repository.**

     **Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

     a. In the repositories table, click the row of the repository that contains the image you want to view.
The **Repository Details** page appears with an overview description of the repository. On the **Repository Details** page, the **Container Images** table appears, listing each image stored in the repository.

b. In the **Container Images** table, click an image row to view additional details.

    The **Tags** page appears.

c. In the **Container Tag** table, click a row to expand the **Activity Log** details plane for that tag.

   **Tip**: In the top navigation bar, click a link in the breadcrumb trail to return to a previous page.

- **Delete an image repository.**

   **Required Tenable.io Vulnerability Management User Role**: Scan Operator, Standard, Scan Manager, or Administrator

a. In the repositories table, click the row of the repository you want to delete.

   The **Repository Details** page appears.

b. In the details section, next to **ACTIONS**, click the **X** button.

   A confirmation window appears.

c. Click **Delete** to confirm.

   **Tip**: In the top navigation bar, click a link in the breadcrumb trail to return to a previous page.
Delete an Image in CS

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable.io Container Security

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Note:** The data Tenable.io Container Security retains when you import an image depends on the import method you use.

- **Docker command** or connector – Tenable.io Container Security retains the image itself, as well as all metadata associated with the image (e.g., image layers, software packages on the image, etc.).

- **Tenable.io CS Scanner** – Tenable.io Container Security retains only the metadata associated with the image. When you delete the image, Tenable.io Container Security removes the entire image and all image metadata.

To delete an image:

1. In the Statistics section of the Container Security dashboard, click the Images widget.

   The Images page appears. This page contains a table that lists the images Tenable.io Container Security has imported and scanned.

2. In the images table, click the × button next to the image you want to delete.

   A Confirm Deletion window appears.

3. Click Delete to confirm the deletion.

   Tenable.io Container Security removes the image and all the vulnerabilities associated with that image.
Manage CS Policies

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Tenable.io Container Security policies allow you to configure the rules that Tenable.io Container Security refers to when it identifies the severity of vulnerabilities in your container images.

When you set a policy in Tenable.io Container Security, the scanner detects any images that meet the conditions set in that policy and labels those images as false.

You can perform the following actions to manage your policies in Tenable.io Container Security:

- Add a CS Policy
- CS Policy Condition Settings
- Edit a CS Policy
- Delete a CS Policy
Add a CS Policy

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable.io Container Security

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

To add a policy in Tenable.io Container Security:

1. In the upper-left corner, click the button.
   The left navigation plane appears.

2. In the left navigation plane, in the **Container Security** section, click **Policies**.
   The **Policies** page appears and displays the policies table.

   **Note:** The policies table lists your policies in order of priority, as determined by Tenable.io Container Security.

3. In the upper-right corner, click **Create Policy**.
   The **New Policy** plane appears.

4. In the policy name text box, type a meaningful name for the policy.

5. In the **Repositories** section, select the repositories where Tenable.io Container Security applies the policy:
   - To apply the policy to all repositories, select **All Repositories**.
   - To apply the policy to one repository:
     a. Select **Specific Repository**.
     b. In the drop-down box, type the name of the repository where you want to apply the policy.
     c. Select the repository.

6. In the **Conditions** section, set the **condition** that triggers the policy.
7. Click **Create Policy**.

The new policy appears on the **Policies** page in the policies table.

**Tip:** In the top navigation bar, click a link in the breadcrumb trail to return to a previous page.

**Note:** By default, the system assigns the policy the highest priority (1). If you want to modify the priority setting, edit the policy.
Edit a CS Policy

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable.io Container Security

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

To edit a policy in Tenable.io Container Security:

1. In the upper-left corner, click the ☐️ button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Container Security** section, click **Policies**.

   The **Policies** page appears and displays the policies table.

   **Note:** The policies table lists your policies in order of priority, as determined by Tenable.io Container Security.

3. Click the policy you want to edit.

   The **Edit Policy** plane appears.

4. In the **Priority** box, type a number representing the priority for the policy.

   Tenable.io Container Security evaluates container images against policies in the priority order you specify.

   If you type a priority number that is already associated to another policy, the system accepts the new priority number and lowers the priority numbers for all policies below it.

5. In the **Repositories** section, select the repositories where Tenable.io Container Security applies the policy:

   - To apply the policy to all repositories, select **All Repositories**.
   - To apply the policy to one repository:
a. Select **Specific Repository**.

b. In the drop-down box, type the name of the repository where you want to apply the policy.

c. Select the repository.

6. In the **Conditions** section, set the **condition** that triggers the policy.

7. Click **Save**.

Tenable.io Container Security saves your changes and displays the updated information on the **Policies** page.

**Tip:** In the top navigation bar, click a link in the breadcrumb trail to return to a previous page.
Delete a CS Policy

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable.io Container Security

**Required Tenable.io Vulnerability Management User Role:** Scan Manager or Administrator

To delete a policy in the policies table:

1. In the **Statistics** section of the **Container Security** dashboard, click the **Policies** widget.

   The **Policies** page appears. This page contains a table that lists the policies Tenable.io Container Security uses to evaluate container images.

   The table lists the policies in order of priority, as determined by Tenable.io Container Security.

2. In the policies table, click the $\times$ button next to the policy you want to delete.

   **Tip:** Roll over the policy row to reveal the $\times$ button for that policy.

3. Click **Delete** to confirm the deletion.

To delete a policy while viewing the policy configuration:

1. In the **Statistics** section of the **Container Security** dashboard, click the **Policies** widget.

   The **Policies** page appears. This page contains a table that lists the policies Tenable.io Container Security uses to evaluate container images.

   The table lists the policies in order of priority, as determined by Tenable.io Container Security.

2. In the policies table, click the row of the policy you want to delete.

   The **Edit Policy** plane appears.

3. In the **Actions** section, click the $\times$ button.

4. Click **Delete** to confirm the deletion.
**Tip:** In the top navigation bar, click a link in the breadcrumb trail to return to a previous page.
You can set one of the following conditions to trigger a policy in Tenable.io Container Security:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| CVSS   | To set the maximum CVSS value that triggers the policy:  
  1. Click **Max CVSS Value**.  
  2. Select an operator from the drop-down box.  
  3. Type the CVSS trigger value. |
| CVE    | To set a CVE or CVEs that trigger the policy:  
  1. Click **CVE**.  
  2. In the text box, type one or more CVE values in decimal format (0.0) in a comma-separated list. |
| Malware| To set the policy to trigger on malware:  
  1. Click **Malware**.  
  2. Select **True** in the drop-down box. |
Risk Metrics in CS

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

Tenable.io Container Security uses the metrics described below to categorize your images and containers on the Tenable.io Container Security dashboard.

Image Risk

Tenable.io Container Security assigns all vulnerabilities in an image a static severity category based on the vulnerability's CVSSv2 score.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>The vulnerability's CVSSv2 score is between 9.0 and 10.0.</td>
</tr>
<tr>
<td>High</td>
<td>The vulnerability's CVSSv2 score is between 7.0 and 8.9.</td>
</tr>
<tr>
<td>Medium</td>
<td>The vulnerability's CVSSv2 score is between 4.0 and 6.9.</td>
</tr>
<tr>
<td>Low</td>
<td>The vulnerability's CVSSv2 score is between 0.1 and 3.9.</td>
</tr>
<tr>
<td>Unscored</td>
<td>Tenable.io Container Security has not yet determined the vulnerability's risk score.</td>
</tr>
</tbody>
</table>

Container Risk

Tenable.io Container Security calculates a container's overall risk score by determining which vulnerability on the container has the highest CVSSv2 score, then rounding that score to the nearest whole number.

For example, if the highest risk score for a vulnerability on a container is 9.2, Tenable.io Container Security assigns the entire container a risk score of 9.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unscanned</td>
<td>The container was created from an image that Tenable.io Container Security has never scanned for vulnerabilities.</td>
</tr>
<tr>
<td>Risk</td>
<td>Tenable.io Container Security scanned the image and container and assigned a risk score of 0-7.</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Low/Medium</td>
<td>Tenable.io Container Security scanned the image and container and assigned a risk score of 0-7.</td>
</tr>
<tr>
<td>High Risk</td>
<td>Tenable.io Container Security scanned the image and container and assigned a risk score of 8-10.</td>
</tr>
</tbody>
</table>
View CS Data Usage

The following feature is not supported in Tenable.io Federal Risk and Authorization Management Program (FedRAMP) environments.

**Required Additional License:** Tenable.io Container Security

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

Tenable.io Container Security displays your data capacity by used and available data in the **Usage** widget on the Container Security dashboard.

The **Usage** widget categorizes your data by licensed container images or gigabytes (GB), depending on which metric your license specifies. For more information about your license metrics, contact your Tenable representative.

To view your data usage:

1. In the Container Security dashboard, locate the **Usage** widget.

2. View the following details about your data usage:

<table>
<thead>
<tr>
<th>Widget Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Licensed Space</strong> or <strong>Licensed</strong>&lt;br&gt;<strong>Images</strong>, depending on your licensing scheme</td>
<td>The amount of data licensed to your account.</td>
</tr>
<tr>
<td><strong>Licensed Space Limit</strong> or <strong>Licensed Images Limit</strong>, depending on your licensing scheme</td>
<td>The amount of licensed data still available.</td>
</tr>
</tbody>
</table>
| **Space used** or **Licensed**<br>**Images used**, depending on your licensing scheme | The amount of licensed data already in use, displayed as a percentage of your licensed data limit. To calculate the data in use, Tenable.io Container Security:  
  - Identifies each image by the combination of con-
- It includes only the three most recent tags of the image against your licensed usage.

As a result, the **Image widget** may display an image count that does not match the amount of used licensed data the **Usage widget** displays.

For example, if your licensed image limit is 20, and you have 10 images already in use, your **Licensed Images used** percentage is 50%.
Dashboard Synchronization in Classic and New Interface

When you add a dashboard in the new interface, the new dashboard also appears in the list of dashboards in the classic interface. In turn, when you add a dashboard in the classic interface, the new dashboard also appears in the list of dashboards in the new interface. Any modifications you make to a dashboard in one interface automatically appear in the corresponding dashboard of the other interface.

Widget order can differ when a dashboard synchronizes from the new to classic interface. If you change the widget order for a dashboard in the new interface, the changed order does not synchronize in the dashboard in the classic interface. You must manually re-order widgets in the classic interface.

Tenable.io synchronizes dashboards when you perform the following actions in the new interface:

- Create a Dashboard
- Delete a Dashboard
- Duplicate a Dashboard
- Manage Widgets
- Rename a Dashboard
- Add a Widget to a Dashboard
- Create a Custom Widget
- Delete a Widget from a Dashboard
- Delete a Widget from the Widget Library
- Duplicate a Widget
- Rename a Widget
View the Dashboards Page

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

Tenable.io updates dashboard data every time you run a scan.

To view the Dashboards page:

1. Access the **Dashboards** page in one of the following ways:
   - On any **Tenable-provided** dashboard page, click the **Dashboards** button.
   - On any other page, do the following:
     a. In the upper-left corner, click the **button.
        
        The left navigation plane appears.
     b. In the left navigation plane, click **Dashboards**.

   The **Dashboards** page appears. The page contains tiles that represent:
   - Tenable-provided dashboards
   - Dashboards you have created
   - Dashboards that other users have shared with you

2. Do any of the following:
   - In the upper-left corner, use the **Search** bar to search for specific dashboards.
   - In the upper-right corner, use the drop-down to change the order in which dashboards appear on the **Dashboards** page.
   - Click the **Shared with Me** tab to view dashboards that have been **shared** with you.
     - On any shared dashboard, roll over the **icon to view the user that shared the dashboard with you.
• Roll over individual tiles to reveal additional information.

• **Toggle** between the grid and list view.

• **Set** a default dashboard.

• Click a dashboard tile to **view** the individual dashboard.
# Tenable-Provided Dashboards

On the **Dashboards** page, Tenable.io displays dashboards in the following order:

1. Tenable-provided dashboards
2. Dashboards you create and dashboards that have been shared with you.

**Note:** You can change the order in which dashboards appear by using the drop-down in the upper-right corner of the **Dashboards** page.

The Tenable-provided dashboards you see depend on the **licenses** you have, but can include the following:

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Management Overview</td>
<td>Tenable.io Vulnerability Management</td>
</tr>
<tr>
<td>Asset View</td>
<td>Tenable.io Vulnerability Management</td>
</tr>
<tr>
<td>Lumin</td>
<td>Lumin</td>
</tr>
<tr>
<td>Container Security</td>
<td>Tenable.io Container Security</td>
</tr>
<tr>
<td>Web Application Scanning</td>
<td>Tenable.io Web Application Scanning</td>
</tr>
</tbody>
</table>

**Note:** You can export the **Vulnerability Management Overview** and **Asset View** dashboard landing pages, or export individual widgets on those dashboards. For more information, see [Export a Full Dashboard](#) and [Export an Individual Dashboard Widget](#).

**Note:** If your dashboard fails to show data, you may be filtering the dashboard by a target group with too many targets. Tenable recommends limiting the number of targets in any individual target group.
Export a Full Dashboard Landing Page

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

In Tenable.io, you can export the following dashboard landing pages:

- [Vulnerability Management Overview](#)
- [Asset View](#)
- [Lumin](#)
- [Tenable.io Web Application Scanning](#)

To export a full dashboard landing page:

1. [View](#) the dashboard page you want to export.
2. In the upper-right corner, click [Export](#).
   
   A drop-down menu appears.

3. From the drop-down menu, select one of the following options:
   - Click [PDF](#) to export the dashboard in PDF format.
   - Click [PNG](#) to export the dashboard in PNG format.
   - Click [JPG](#) to export the dashboard in JPG format.

   An [In Progress](#) message appears.

Once the export completes, a [Success](#) message appears and Tenable.io downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.
Export an Individual Dashboard Widget

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

In Tenable.io, you can export individual widgets from the following dashboard landing pages:

- [Vulnerability Management Overview](#)
- [Asset View](#)
- [Lumin](#)
- [Tenable.io Web Application Scanning](#)

To export an individual dashboard widget:

1. **View** the dashboard page that contains the widget you want to export.

2. In the header of the widget you want to export, click the ••• button.

   A drop-down menu appears.

3. From the drop-down menu, select one of the following options:

   - Click **PDF** to export the dashboard in PDF format.
   - Click **PNG** to export the dashboard in PNG format.
   - Click **JPG** to export the dashboard in JPG format.

   An **In Progress** message appears.

Once the export completes, a **Success** message appears and Tenable.io downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.
View an Individual Dashboard

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

Tenable.io Vulnerability Management updates dashboard data every time you run a scan. Tenable.io Web Application Scanning updates dashboard data every time your scan data changes. However, after Tenable.io Web Application Scanning completes a scan, it can take up to 10 minutes for the scan results to appear on the dashboard.

To view an individual dashboard:

1. **View** the **Dashboards** page.

2. Do one of the following:
   - In grid view, roll over the tile for the dashboard you want to view.
     Dashboard information and options overlay the dashboard tile.
   - In list view, roll over the thumbnail dashboard image for the dashboard you want to view.
     Dashboard options overlay the thumbnail dashboard image.

3. **Click** **View**.
   The page for that dashboard appears.

4. Do one of the following:
   - Change the dashboard you are viewing:
     a. In the upper-left corner of the page, next to the dashboard name, click the ▼ button.
        A drop-down menu appears.
     b. Select the dashboard you want to view.
        Tenable.io displays the selected dashboard.
   - Roll over individual widgets to reveal additional information.
   - Click on widget elements to drill down into details behind the data.
View the Dashboard Template Library

Required Tenable.io Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

In the new interface, the Template Library provides a selection of Tenable-provided dashboards.

Tip: For detailed descriptions of Tenable.io dashboard templates, see the Tenable.io Dashboards blog post.

To view the dashboard template library in the new interface:

1. View the Dashboards page.
2. Click ☺ New Dashboard.
   A list of options appears.
3. Click Template Library.
   The Template Library page appears.

On the Template Library page, you can:

- Sort the Template Library page:
  a. In the upper-right corner of the page, click the ▼ button in the drop-down box.
  b. Select the criteria by which you want to sort the page.

- In the upper-left corner, use the Search bar to search for specific dashboards.

- Toggle between the grid and list view.

- Preview a dashboard.

- Create a dashboard.
Create a Dashboard

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

To create a dashboard in the new interface:

1. **View** the **Dashboards** page.
2. Click **New Dashboard**.

   A list of options appears.

3. Do one of the following:

   To create a dashboard from a template:
   
   a. Click **Template Library**.

   The **Template Library** page appears.

   b. In the library, locate the template you want to use.

   c. Roll over the template.

   An overlay of template information and options appears.

   d. (Optional) To preview the dashboard template, click **Preview**. For more information, see **Preview a Dashboard**.

   e. Click **Add**.

   An **Added dashboard to Dashboards** confirmation message appears, and the new dashboard appears on the **Dashboards** page with the name **Copy of selected dashboard**.

   To create a custom dashboard:

   Click **Custom Dashboard**.

   a. The **Edit Dashboard** page appears.
b. Name the dashboard:
   a. Click the name of the dashboard.
      The name becomes an editable text box.
   b. Type a name for the dashboard.
   c. Click the ✓ button to confirm the name change.
      Tenable.io saves the updated name.

c. Add a dashboard description:
   a. Click the dashboard description.
      The description becomes an editable text box.
   b. Type a description for the dashboard.

d. Add widgets to the dashboard:
   a. In the upper-right corner of the page, click Add Widgets.
      A menu appears.
   b. Do one of the following:
      
      • To add a widget from a template, click Template Widget.
         The Widgets page appears.
         ◦ Select the widget as described in Add a Widget to a Dashboard.
      
      • To add a custom widget, click Custom Widget.
         The Create Widget page appears.
         ◦ Configure the custom widget as described in Create a Custom Widget.

e. Add dashboard filters:
a. In the upper-right corner of the page, click Edit Filter.

The Filter plane appears.

Note: The Edit Filter option does not appear if there are no widgets added to the dashboard.

b. Configure your dashboard filters as described in Filter a Dashboard.

f. (Optional) Reorder widgets on the dashboard:
   a. Roll over widget you want to move.
   b. Press and hold the mouse button to select the widget.
      The edges of the widget become defined and exhibit a raised appearance.
   c. Holding the mouse, drag the widget to the new location.
   d. Release the mouse button to drop the widget in the new location.

g. (Optional) Delete the dashboard:
   o In the lower-left corner of the page, click Delete Dashboard.

Tenable.io discards the newly created dashboard.

What to do next:

• Manage Dashboards
Preview a Dashboard

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

When creating a new dashboard from a template, you can preview the dashboard before adding it to the Dashboards page.

To preview a dashboard:

1. **Create** a dashboard.

2. In the **Template Library**, roll over the template you want to preview.
   - An overlay of template information and options appears.

3. Click **Preview**.
   - A preview of the dashboard appears.

4. To exit the preview, in the top navigation bar, click a link in the breadcrumb trail to return to the Template Library, or the Dashboards page.

5. To add the template to the Dashboards page, click **Add to Dashboards**.
   - An **Added dashboard to Dashboards** confirmation message appears, and the new dashboard appears on the Dashboards page with the name **Copy of selected dashboard**.
Manage Dashboards

This section contains the following topics related to managing dashboards in the new interface:

- **Toggle the Grid and List Dashboards View**
- **Edit a Dashboard**
- **Set a Default Dashboard**
- **Rename a Dashboard**
- **Duplicate a Dashboard**
- **Filter a Dashboard**
- **Share a Dashboard**
- **Export an Individual Dashboard Widget**
- **Export a Dashboard**
- **Delete a Dashboard Export Download**
- **Delete a Dashboard**
Toggle the Grid and List Dashboards View

Required Tenable.io Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

When viewing the Dashboards page, you can toggle between a grid view and a list view.

To toggle the grid and list dashboards view:

1. **View** the Dashboards page.

2. To view the Dashboards page in the grid view, in the upper-right corner of the page, click the button.

   The Dashboards page appears in the grid view.

3. To view the Dashboards page in the list view, in the upper-right corner of the page, click the button.

   The Dashboards page appears in the list view.
Edit a Dashboard

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To edit a dashboard in the new interface:

1. Do one of the following:
   
   • Access the **Edit Dashboard** page via the **Dashboards** page:
     
     a. **View** the **Dashboards** page.
     
     b. In the dashboard header, click the : button.
        
        A drop-down list appears.
     
     c. Click **Edit**.
   
   • Access the **Edit Dashboard** page via an individual dashboard:
     
     a. **View** the dashboard you want to edit.
     
     b. In the dashboard header, click the **More** button.
        
        A drop-down appears.
     
     c. Click **Edit dashboard**.

     The **Edit Dashboard** page appears.

2. On the **Edit Dashboard** page, do any of the following:

   • Rename the dashboard:
     
     a. Click the name of the dashboard.
        
        The name becomes an editable text box.
     
     b. Type a new name for the dashboard.
c. Click the ✔️ button to confirm the name change.

Tenable.io saves the name.

• Edit the dashboard description:
  a. Click the dashboard description.

  The description becomes an editable text box.
  b. Type a new description for the dashboard.

• Edit the dashboard filters:
  a. In the upper-right corner of the page, click ✂️ Edit Filter.

  The Filter plane appears.
  b. Configure your dashboard filters as described in Filter a Dashboard.

• Add widgets to the dashboard:
  a. In the upper-right corner of the page, click ✡️ Add Widgets.

  A menu appears.
  b. Do one of the following:

    • To add a widget from a template, click Template Widget.

      The Widgets page appears.
      ◦ Select the widget as described in Add a Widget to a Dashboard.

    • To add a custom widget, click Custom Widget.

      The Create Widget page appears.
      ◦ Configure the custom widget as described in Create a Custom Widget.

• Reorder widgets on the dashboard:
a. Roll over the top of the widget until the move cursor appears.

b. Click and drag the widget to the desired location.

• Resize the widgets on the dashboard:
  a. Roll over the lower-right corner of the widget until the resize cursor appears.
  b. Click and drag the widget to the desired size.

  The widgets shift to accommodate the new widget size.

• Delete the dashboard:
  o In the lower-left corner of the page, click Delete Dashboard.

  Tenable.io removes the dashboard from the Dashboards page.

3. Click Done Editing.

  You return to the selected dashboard and Tenable.io applies your changes.
**Set a Default Dashboard**

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

The default dashboard acts as the landing page for the new interface. You can set any dashboard as the default dashboard.

If you do not set a default dashboard, Tenable.io uses the Tenable-provided **Vulnerability Management Overview** dashboard as the default.

When you set a dashboard as default, on the **Dashboards** page, the **Default** label appears in the header of the dashboard tile.

**Note:** If you delete a dashboard set as default, the product Tenable-provided dashboard becomes the default.

To set a default dashboard in the new interface:

1. **View** the **Dashboards** page.

2. In the dashboard header, click the **button.

   A drop-down list appears.

3. Select **Make Default**.

   A **Successfully set as default dashboard** confirmation message appears, and Tenable.io sets the dashboard as the default.

**Note:** You may have to log out and log back in to see the updated default dashboard.
Rename a Dashboard

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

To rename a dashboard in the new interface:

1. **View** the dashboard you want to rename.

2. On the dashboard page, roll over the dashboard name.
   
   The name becomes highlighted and displays a **edit** button.

3. Click the **edit** button or double click the name.
   
   The name field becomes a text box.

4. Enter a new name for the dashboard.

5. **Click the **✓** button to confirm the name change.**
   
   A confirmation appears at the top of the page.

   The new name appears.
Duplicate a Dashboard

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

To duplicate a dashboard in the new interface:

1. **View** the **Dashboards** page.
2. In the dashboard header, click the ✡ button.
   
   A drop-down list appears.
3. Select **Duplicate**.

   A **Successfully copied the dashboard** confirmation message appears, and Tenable.io copies the dashboard on the **Dashboards** page.
Filter a Dashboard

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

In the new interface, the filter option allows you to display only widgets with a specific configuration.

Filters configured at the dashboard level apply to all widgets within that dashboard.

**Note:** You can apply configurations to individual widgets. The widget-level configuration takes precedence over dashboard-level configuration.

To filter a dashboard in the new interface:

1. **View** the dashboard you want to filter.
2. In the dashboard header, click the **More** button.
   
   **Note:** The **More** button is not available on Tenable-provided dashboards.

   A drop-down appears.

3. Click **Filter**.

   The **Filter** plane appears.

4. In the **Select Filter Type** drop-down, select the assets you want the dashboard to analyze. See the table below for options and requirements.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Assets</td>
<td>(Default) This option includes all of the assets in the dashboard.</td>
<td>This is the default option and includes all assets in the dashboard. There is not a requirement for this option.</td>
</tr>
<tr>
<td>Target Group</td>
<td>This option only includes assets in a specific target</td>
<td>When this option is selected an additional field for <strong>Select Target Groups</strong> is added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------------------------------------------------</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Select</strong></td>
<td>The desired target group from the drop-down list.</td>
<td></td>
</tr>
<tr>
<td><strong>Custom</strong></td>
<td>This option only includes assets with a specific host name, IP</td>
<td>When this option is selected a text box appears. Enter one or</td>
</tr>
<tr>
<td></td>
<td>address, FQDN, or CIDR.</td>
<td>more of the custom option formats (host name, IP address, FQDN,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>or CIDR). Multiple items must be separated by a comma.</td>
</tr>
</tbody>
</table>

5. Click **Apply**.

The \( \checkmark \) icon displays in the header of all of the dashboard widgets.

6. In the widgets section, roll over the \( \checkmark \) icon to view the added filter.
Share a Dashboard

Tenable.io users can share a dashboard with one or more users, or one or more user groups. Shared dashboards appear automatically for the user(s) or group(s) with which they are shared.

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Note:** Dashboards that are shared with you cannot be edited. You can, however, duplicate or delete a dashboard that is shared with you.

**Note:** Dashboards are not automatically re-shared with a user after they have been updated. For example: User A shares a dashboard with User B. User A then makes a change to the dashboard. To see the updated dashboard, User A must re-share the dashboard with User B.

**Note:** Shared content may appear differently to the users with which it is shared based on the access group to which they belong.

To share a dashboard in the new interface:

1. Do one of the following:
   - To share a dashboard via the **Dashboards** page:
     - a. **View** the **Dashboards** page.
     - b. In the dashboard header, click the button.
     - A drop-down list appears.
     - c. Select **Share**.
   - To share a dashboard via an individual dashboard:
     - a. **View** the dashboard you want to share.
     - b. In the upper-right corner, click **Share**.

     The **Share** plane appears.

2. Do one of the following:
• To share the dashboard with all users, select the **All Users** check box.

• To share the dashboard with specific users or user groups, from the drop-down box, select the user(s) or user group(s) with which you want to share the dashboard.

  **Tip:** You can share with multiple users or user groups.

3. Click **Share**.

A **Dashboard shared successfully** message appears. Tenable.io shares the dashboard with the designated user(s) or user group(s) and sends an email indicating that a dashboard has been shared with them.
Export a Dashboard

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

In the new interface, the export feature allows you to export dashboard data in PDF detailed PDF formats. You can create dashboard exports on demand, or you can schedule automated exports to specified recipients.

**Note:** By default, the following dashboards support PDF-Detailed exports:

- Executive Summary
- Exploitable by Malware
- Exploitable Framework Analysis
- Measuring Vulnerability Management
- Mitigation Summary
- Outstanding Remediation Tracking
- Prioritize Assets
- Vulnerabilities by Common Ports
- Vulnerability Management
- Web Services

**Note:** While you cannot export the Vulnerability Management Overview and Asset View dashboards, you can export their associated landing pages, or export individual widgets on those dashboards. For more information, see Export a Full Dashboard Landing Page and Export an Individual Dashboard Widget.

To export a dashboard as a PDF:

You can use the Export PDF feature to share customized dashboards externally. The exported PDF is a generated report of the selected dashboard.

To export a PDF:
1. **View** the dashboard you want to export.

2. In the upper-right corner, click **Export**.

   A drop-down list appears.

3. Click **PDF** or, where available, **PDF - Detailed**.

   **Note:** The PDF report contains the displayed information for the selected dashboard. The information that you see on the screen is the information that will be included in the report.

   The PDF - Detailed report has in-depth information, including vulnerability details, that goes beyond the items displayed.

   **Note:** If you select **PDF - Detailed** and there are user-created filters applied to one or more widgets on the dashboard, a **Confirm Export** message appears indicating that Tenable.io does not apply user-created filters to any additional chapters. Click **confirm** to continue with the export.

An **Export in Progress** confirmation message appears.

The export request and status appears in the **Downloads** section on the **Exports** plane.

When the export completes, Tenable.io downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

**To schedule a dashboard export:**

The **Schedule Export** option allows you to export a dashboard at specified times.

**To schedule an export:**

1. Do one of the following:

   - Access the **Schedule Export** plane via the **Dashboards** page:
     a. **View** the **Dashboards** page.
     b. In the dashboard header, click the **Dashboard** button.

       A drop-down list appears.

     c. Click **Schedule Export**.
• Access the **Schedule Export** plane via an individual dashboard:
  
a. **View** the dashboard you want to export.

b. In the upper-right corner, click **Export**.

A drop-down list appears.

c. From the drop-down list, click **Schedule**.

The **Schedule Export** plane appears.

2. Do one of the following:

• If you have never exported and/or scheduled an export for the dashboard, the **Schedule** options automatically appear.

• If you have already exported the dashboard, in the **Schedule** section, click ✖ Add New.

The **Schedule** options appear.

• If you have already scheduled an export for the dashboard, you cannot create another one. You must first **cancel** the scheduled dashboard export.

3. Select **PDF** or, where available, **PDF - Detailed**.

   **Note:** The PDF report contains the displayed information for the selected dashboard. The information that you see on the screen is the information that will be included in the report.

   The **PDF - Detailed** report has in-depth information, including vulnerability details, that goes beyond the items displayed.

   **Note:** If you select **PDF - Detailed** and there are user-created filters applied to one or more widgets on the dashboard, a **Confirm Export** message appears indicating that Tenable.io does not apply user-created filters to any additional chapters. Click **Confirm** to continue with the export.

4. In the **Schedule** section, set the following parameters:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the scheduled export.</td>
</tr>
<tr>
<td>Start Date and Time</td>
<td>The date and time that you want the export to begin.</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------</td>
</tr>
<tr>
<td>Repeat</td>
<td>The frequency that you want the export to be sent:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Daily</strong> – The export occurs daily at the time specified.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Weekly</strong> – The export occurs every week on the same day at the time specified (e.g., Weekly on Tuesday).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Monthly</strong> – The export occurs once a month on the day of the week and time specified (e.g. Monthly on Last Tuesday)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Custom</strong> – The export occurs at a custom interval. If you select <strong>Custom</strong>, additional options appear:</td>
</tr>
<tr>
<td></td>
<td>a. In the <strong>Repeat Every</strong> section, in the drop-down, select how often you want the export to repeat. For example, if you want the export to repeat every 2 days, then in the first drop-down box, select <strong>2</strong> and in the the second drop-down box, select <strong>Days</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Does not Repeat</strong> – The export does not repeat.</td>
</tr>
<tr>
<td>PDF Encryption</td>
<td>Specifies the export as encrypted or unencrypted.</td>
</tr>
<tr>
<td></td>
<td>If you select <strong>Encrypted</strong>, an <strong>Encryption Password</strong> box appears.</td>
</tr>
<tr>
<td></td>
<td>Type the password you want to use to encrypt the export file.</td>
</tr>
</tbody>
</table>

**Note:** Once you save the scheduled export, you cannot edit the PDF Encryption parameter. Instead, you must create a copy of the dashboard, create a scheduled export, and then select the desired encryption parameter.

| Add Recipients      | (Optional) The email address for the person that will receive the report. You can specify multiple email addresses as a comma-delimited list. |

5. Click **Schedule**.

The scheduled export appears in the **Schedule Export** plane.
Download an Available Export Download

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can view or download an available dashboard export download at any time from the **Schedule Export** plane. For more information about exporting a dashboard, see **Export a Dashboard**.

To view or download a dashboard export download:

1. Do one of the following:
   
   - Access the **Schedule Export** plane via the **Dashboards** page:
     
     a. **View** the **Dashboards** page.
     
     b. In the dashboard header, click the : button.
     
     A drop-down list appears.
     
     c. Click **Export**.
   
   - Access the **Schedule Export** plane via an individual dashboard:
     
     a. **View** the dashboard with the export you want to download.
     
     b. In the upper-right corner, click **Export**.
     
     A drop-down list appears.
     
     c. From the drop-down list, click **Schedule**.

     The **Schedule Export** plane appears.

2. In the **Downloads** section, next to the export download you want to download, click the : button.

   Tenable.io downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.
Delete a Scheduled Dashboard Export Configuration

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can delete a scheduled dashboard export configuration at any time from the **Schedule Export** plane. For more information about configuring a dashboard export, see [Export a Dashboard](#).

To delete a scheduled dashboard export configuration:

1. Do one of the following:
   - Access the **Schedule Export** plane via the **Dashboards** page:
     a. **View** the **Dashboards** page.
     b. In the dashboard header, click the : button.
        
        A drop-down list appears.
     c. Click **Export**.
   - Access the **Schedule Export** plane via an individual dashboard:
     a. **View** the dashboard for which you want to delete a scheduled export.
     b. In the upper-right corner, click **Export**.
        
        A drop-down list appears.
     c. From the drop-down list, click **Schedule**.
        
        The **Schedule Export** plane appears.

2. In the **Schedule** section, roll over the scheduled export configuration you want to delete.

3. Click the ☐ button.

   A **Confirm Deletion** message appears.

4. Click **Confirm**.

   A **Successfully deleted export configuration** message appears and Tenable.io removes the export configuration from the **Schedule** section of the **Schedule Export** plane.
Delete a Dashboard Export Download

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can delete a dashboard export download at any time from the Schedule Export plane. For more information about exporting a dashboard, see Export a Dashboard.

To delete a dashboard export download:

1. Do one of the following:
   - Access the Schedule Export plane via the Dashboards page:
     a. View the Dashboards page.
     b. In the dashboard header, click the button.
     A drop-down list appears.
     c. Click Export.
   - Access the Schedule Export plane via an individual dashboard:
     a. View the dashboard for which you want to delete an export.
     b. In the upper-right corner, click Export.
     A drop-down list appears.
     c. From the drop-down list, click Schedule.

   The Schedule Export plane appears.

2. In the Downloads section, roll over the export download you want to delete.

3. Click the button.

   A Confirm Deletion message appears.

4. Click Delete.

   A Download deleted successfully message appears and Tenable.io removes the export download from the Schedule Export plane.
Delete a Dashboard

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

To delete a dashboard:

1. Do one of the following:
   - **Delete a dashboard from the Dashboards page:**
     a. View the Dashboards page.
     b. In the dashboard tile header, click the button.
   - **Delete a dashboard from the individual dashboard:**
     a. View the dashboard page you want to delete.
     b. In the dashboard header, click the More ▼ button.

   A drop-down list appears.

2. Click **Delete**.

   A **Confirm Deletion** confirmation message appears.

3. Click **Delete**.

   A **Successfully deleted the dashboard** confirmation message appears and Tenable.io removes the dashboard from the Dashboards page.
Manage Widgets

In the new interface, you can use the widget library to create and edit widgets to use across your dashboards.

To manage widgets in the widget library:

- View the Widget Library
- Create a Custom Widget
- Edit a Custom Widget
- Add a Widget to a Dashboard

On your dashboards, you can further configure widgets to modify your dashboards.

To manage widgets on a dashboard:

- Configure a Widget
- Duplicate a Widget
- Rename a Widget
- Delete a Widget from a Dashboard
View the Widget Library

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

In the new interface, the widget library provides a selection of Tenable-provided widgets to quickly add to your template-based or custom dashboard.

**Note:** The Tenable-provided **Vulnerability Trending** widget is not available in the widget library. All other Tenable-provided widgets appear in the widget library.

To view the widget library in the new interface:

1. **View** the **Dashboards** page.
2. In the upper-right corner of the page, click the **Widget Library** button.

   The **Widgets** page appears.
3. (Optional) In the upper-left corner of the page, click the tab for the dashboard widgets you want to view. For example, if you want to only widgets associated with Vulnerability Management, click the **Vulnerability Management** tab.

   **Note:** The tabs that appear on the **Widgets** page depend on the **licenses** (e.g., Lumin, Tenable.io Web Application Scanning) you have enabled in Tenable.io.

On the **Widgets** page you can:

- Sort the **Widgets** page:
  a. In the upper-right corner of the page, click the **button in the drop-down box.
  b. Select the criteria by which you want to sort the widgets page.

- In the upper left corner, use the **Search** bar to search for specific widgets.

- **Toggle** between the grid and list view.
• **Add** the widget to a dashboard.

• **Delete** a widget from the widget library.
When viewing the Widgets page, you can toggle between a grid view and a list view.

To toggle the grid and list widgets view:

1. View the Widgets page.

2. To view the Widgets page in the grid view, in the upper-right corner of the page, click the button.
   
The Widgets page appears in the grid view.

3. To view the Widgets page in the list view, in the upper-right corner of the page, click the button.
   
The Widgets page appears in the list view.
Delete a Widget from the Widget Library

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Note:** You can only delete custom widgets. You cannot delete pre-configured vulnerability management widgets.

To delete a custom widget:

1. **View** the widget library.

2. Click the **My Widgets** tab.

   All user-created widgets appear.

3. In the header of the widget you want to delete, click the button.

   A drop-down menu appears.

4. Click **Delete**.

   A confirmation window appears.

5. Click **Delete**.

   Tenable.io removes the widget from the widget plane, and a message confirming the deletion appears at the top of the plane.
Create a Custom Widget

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Video:** Custom Widgets in Tenable.io

You can use the custom widget option to create uniquely defined widgets, which you can then add to any user-defined dashboards.

**Note:** When you make updates, the changes also appear in the classic interface. For more information about this sync, see the Dashboard Synchronization in Classic and New Interface page.

To create a custom widget in the new interface:

1. Do one of the following:

   - Create a custom widget via the widget library:
     a. View the widget library.
     b. In the upper-right corner of the page, click the Custom Widget button.

       The Create Custom Widget page appears.

   - Create a custom widget while editing a dashboard:
     a. Edit a dashboard.
     b. In the upper-right corner of the page, click Add Widgets.

       A menu appears.

     c. Click Custom Widget.

       The Create Custom Widget page appears.
2. In the upper-right corner of the page, click **Add Widgets**.

   A menu appears.

3. Click **Custom Widget**.

   The **Widgets** page appears.

4. In the charts section, select the chart type for your custom widget:

   • Table
   • Ring chart (**Vulnerabilities** data set only)
   • Bar chart (**Vulnerabilities** data set only)

5. In the **Data Set** drop-down box, select the type of information Tenable.io uses to update the widget:

   • **Vulnerabilities**
   • **Assets**

   **Note:** If you selected ring chart or bar chart in the charts section, selecting the **Assets** data set will reset the chart selection to a table.

   The chart type, **Data Grouping**, and **Display Fields** options update based on your selection.

6. In the **Data Grouping** drop-down box, select how you want to group the data:

   • **By Plugin** (**Vulnerabilities** data set only)
   • **By Asset** (**Vulnerabilities** data set only)
   • **By CVE** (**Vulnerabilities** data set only)
   • **Asset List** (**Assets** data set only)

7. (Optional) To filter the widget data using filters:
a. Click the ▾ button to expand the filter options.

b. In the drop-down box, select category, operator, and value types.

c. (Optional) Click the ✪ Add button to specify additional filters.

**Note:** If you previously created a tag, it appears in the custom widget's list of filters.

**Note:** If you exceed the current asset query limitation of 5,000, a message appears in your interface. You should refine the query to a smaller set of asset tags.

**Note:** Tag filters are not currently supported in exports.

8. (Optional) To filter the widget data using an existing saved search, in the **Saved Searches** drop-down box, select the saved search you want to use to filter your widget data.

**Note:** If you do not have any saved searches, this option does not appear. To create a new saved search, see **Saved Search**.

9. In the **Name** box, type a name for the custom widget.

In the **Widget Preview**, the title updates automatically.

10. (Optional) In the **Description** box, type a description for the custom widget.

In the **Widget Preview**, the ✡ icon appears and the description hover text updates automatically.

11. Click **Update Preview** to update the widget preview.

**Note:** While **Name**, **Description**, and the chart type all update in the widget preview automatically, all other configuration options refresh after you click **Update Preview**.

12. Click **Save and Exit**.

Tenable.io saves the custom widget to the widget library, and you can add the widget to any user-defined dashboards.
Edit a Custom Widget

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Note:** You cannot edit Tenable-provided widgets.

To edit a custom widget:

1. [View] the widget library.

2. Click the **My Widgets** tab.
   
   All user-created widgets appear.

3. In the upper-right corner of the widget you want to edit, click the ☰ button.
   
   A menu appears.

4. Click **Edit**.
   
   The widget options appear.

5. Edit the widget options.

6. Click **Save and Exit**.
   
   A confirmation appears.

**Note:** A custom widget that was previously included in dashboards before you edited the widget does not update to reflect your edits. To include the edited widget, you must add the widget again as described in Add a Widget to a Dashboard.
Add a Widget to a Dashboard

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

Use the following steps to add a widget to your template-based and custom dashboards in the new interface.

You can add custom widgets, widgets from Tenable-provided dashboards, and other general purpose Tenable-provided widgets.

To add a widget to a dashboard in the new interface:

**Note:** These steps describe how to add a template widget to a dashboard. See custom widgets for information on how to create custom widgets and add them to your dashboard.

1. **View** the widget library.

2. For each widget you want to add:

   a. Do one of the following:

      • Scroll through the list of widgets.
      • Use the **Search** box to find a specific widget.

      **Tip:** You can hover over a widget tile for brief descriptions of each widget. For detailed descriptions about widgets originating from Tenable-provided dashboards, see Tenable-Provided Dashboards.

   b. Roll over the widget you want to add.

      The **Add to Dashboards** button appears.

   c. Click **Add to Dashboards**.

      The **Add to Dashboards** plane appears.
d. In the **Dashboards** drop-down box, select the dashboard or dashboards to which you want to add the widget.

e. Click **Save**.

   Tenable.io adds the widget to the bottom of the appropriate dashboard or dashboards.

f. Click ☑ **Add**.

   Tenable.io adds the widget to the bottom of the appropriate dashboard.

3. Click **Done**.

   You return to the **Dashboards** page.
Configure a Widget

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To configure a widget in the new interface:

1. **View** the dashboard page that contains the widget you want to configure.
2. In the upper-right corner of the widget you want to change, click the button.
   
   A menu appears.
3. Click **Configure**.
   
   The widget summary plane appears.
4. On the widget summary plane, do any of the following:

   - **Rename the widget:**
     
     a. Do one of the following:

     - Click the name of the widget.

     - In the widget summary plane, roll over the widget name and click the button.

     The name field becomes an editable text box.

     b. Type a new name for the widget.

     c. Click the ✓ button to confirm the name change.

     A confirmation message appears at the top of the page, and the new name appears in the widget header.

   - **Edit the widget description:**
a. Do one of the following:
   - Click the widget description.
     - In the widget summary plane, roll over the widget description and click the button.
     The description field becomes an editable text box.
   b. Type a new description for the widget.
   c. Click the button to confirm the change.
     A confirmation message appears at the top of the page, and the new description appears in the widget header.

   - Duplicate the widget:
     - In the Actions row, click the button.
     A confirmation message appears and Tenable.io adds the duplicated widget to the dashboard.

   - Delete the widget from the dashboard:
     a. In the Actions row, click the button.
     A Confirm Deletion message appears.
     b. Click Delete.
     A confirmation message appears and Tenable.io removes the dashboard from the Dashboards page.

   - Apply filters to the widget:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Assets</td>
<td>(Default) This option includes all of the assets in the dashboard.</td>
<td>This is the default option and includes all assets in the dash-</td>
</tr>
<tr>
<td>Target Groups</td>
<td>This option only includes assets in a specific target group.</td>
<td>When this option is selected an additional field for <strong>Select Target Groups</strong> appears. Select the desired target group from the drop-down list.</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Custom</td>
<td>This option only includes assets with a specific host name, IP address, FQDN, or CIDR.</td>
<td>When this option is selected a text box appears. Enter one or more of the custom option formats (host name, IP address, FQDN, or CIDR). Multiple items must be separated by a comma.</td>
</tr>
<tr>
<td>Tags</td>
<td>This option uses tags to filter asset results or vulnerability results.</td>
<td>When this option is selected, a drop down box appears. Select or type the tag name by which you want to filter results. Tenable.io filters the results by the selected tag(s).</td>
</tr>
</tbody>
</table>

**Note:** Tenable.io supports a maximum of 100 filters.

**Note:** Once you apply a filter to a widget, a ✅ icon appears in the widget header. Roll over the ✅ icon to view the applied filter.

5. Click **Apply**.

A confirmation message appears and Tenable.io applies your changes to the widget.
Duplicate a Widget

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To duplicate a widget in the new interface:

1. **View** the dashboard page that contains the widget you want to duplicate.
2. In the upper-right corner of the widget you want to duplicate, click the button.
   A menu appears.
3. Click **Duplicate**.
   The duplicated widget appears at the bottom of the page.
4. (Optional) **Change** the name of the widget.
5. (Optional) Reorder the widget sections.
**Rename a Widget**

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

To rename a widget in the new interface:

1. **View** the dashboard page that contains the widget you want to change.
2. In the upper-right corner of the widget you want to rename, click the ☐️ button.

   A menu appears.

3. Click **Configure**.

   The widget summary plane appears.

4. In the widget summary plane, roll over the widget name.

   The ✂️ button appears next to the name.

5. Click the ✂️ button or double-click the name.

   The name field becomes an editable text box.

6. Type a new name for the widget.

7. Click the ✅ button to confirm the name change.

   A confirmation message appears at the top of the page.

   The new name appears in the widget header.
Delete a Widget from a Dashboard

**Required Tenable.io Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To remove a widget from a dashboard in the new interface:

1. **View** the dashboard page that contains the widget you want to remove.
2. In the upper-right corner of the widget you want to remove, click the button.
   
   A menu appears.
3. Click **Delete**.
   
   Tenable.io prompts you to confirm the removal.
4. Click **Delete**.
   
   A confirmation message appears at the top of the page.

   Tenable.io removes the widget from the dashboard. Remaining widgets adjust to fill the new space.
Dashboards and Workbenches (Classic Interface)

Tenable.io features rich, graphical summaries of scans, scan results, and system activity. Tenable.io updates dashboard data every time you run a scan.

To access the Dashboards page, in the top navigation bar, click Dashboards.

Based on the modules you have activated, you may have access to a number of different workbenches and dashboards. The modules available to you appear in the left navigation bar.

Tenable provides the following workbenches in Tenable.io:

- **Vulnerabilities (Classic Interface)**
- **Assets (Classic Interface)**
- **Health and Status (Classic Interface)**

For information about creating additional dashboards, see Create a Dashboard (Classic Interface).

On the Dashboards page, you can click on a chart in a workbench to display the list of vulnerabilities or assets in the chart. This list changes depending on the filter you apply. For more information, see Filter the Vulnerabilities or Assets Workbench (Classic Interface).

Before you can view any chart, you must read and configure your scan result's privacy. By default, all scan results are set to Private.
Web Applications Workbench (Classic Interface)

Note: This topic describes the Web Applications workbench, which is available only in the classic interface. If you activate the new interface, you can view a snapshot of historical scan data in the workbench, but the snapshot version does not reflect changes you might make to your scan configurations in the new interface.

To view and manage dashboards in the new interface, see WAS Dashboard.

The Web Applications workbench displays data collected by Web Application scans.

The table below describes the charts available on the Web Applications workbench in the classic interface. You can view details about the data in a chart by clicking the chart.
<table>
<thead>
<tr>
<th>Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web Applications: By Plugin</strong></td>
<td></td>
</tr>
<tr>
<td>Current Vulnerabilities</td>
<td>Each number <strong>(Critical, High, Medium, and Low)</strong> represents the vulnerabilities discovered by Web Application scans within the selected time interval and sorted by severity.</td>
</tr>
<tr>
<td>Vulnerabilities Over Time</td>
<td>Vulnerabilities discovered over time by Web Application scans. Each data point on the line graph represents the number of unique vulnerabilities found on a particular day.</td>
</tr>
<tr>
<td>Total Plugins</td>
<td>A list of all the plugins that detected the vulnerabilities that appear on the Web Applications workbench.</td>
</tr>
<tr>
<td><strong>Web Applications: By Application</strong></td>
<td></td>
</tr>
<tr>
<td>Apps Over Time</td>
<td>Applications scanned over time. Each data point on the line graph represents the number of unique applications scanned on a particular day.</td>
</tr>
</tbody>
</table>
PCI ASV (Classic Interface)

Use the PCI ASV workbench to manage PCI ASV attestation requests. For more information, see [Submit a Scan to the PCI ASV Workbench (Classic Interface)](#).
Health and Status (Classic Interface)

The Health & Status workbench is visible to users with the Administrator role and provides quick insight into your organization's historical use of Tenable.io.

The following table contains a description of each chart on the Health & Status workbench.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current License Usage: Assets</td>
<td>Displays the total number of unique assets scanned.</td>
</tr>
<tr>
<td>Current License Usage: Agents</td>
<td>Displays the total number of agents that have been linked.</td>
</tr>
<tr>
<td>Current License Usage: Scanners</td>
<td>Displays the total number of scanners that have been linked.</td>
</tr>
<tr>
<td>Current License Usage: Users</td>
<td>Displays the total number of users that have successfully logged into Tenable.io at least once.</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Scans Per Day</td>
<td>Displays the number of scans launched per day in the last 30 days. Each bar represents all of the scans launched in one day.</td>
</tr>
<tr>
<td>Completed Scans</td>
<td>Displays the number of launched scans that were completed, aborted, or canceled in the last 30 days.</td>
</tr>
<tr>
<td>New Scans</td>
<td>Displays the number of new scans that were scheduled, including on-demand scans in the last 30 days.</td>
</tr>
<tr>
<td>Scheduled Scans</td>
<td>Displays the number of scans that were launched automatically via the scheduling service in the last 30 days.</td>
</tr>
<tr>
<td>On Demand Scans</td>
<td>Displays the number of scans that were launched manually in the last 30 days.</td>
</tr>
</tbody>
</table>
Dashboard Templates (Classic Interface)

The dashboard templates are listed in the left navigation bar. These templates enable you to quickly update and save customized dashboards.

Click on the template name in the Dashboard Templates section to view the different types.

Customize the template by reordering, deleting, or duplicating components.

Tenable.io automatically saves your new, customized dashboard to the My Dashboards section of the left navigation bar when you make a change to a template. For more information on changing templates, see Component Customization.

**Note:** Tenable recommends that you rename a dashboard once you customize it. This practice prevents the confusion of multiple dashboards with the same name. To update, click the button next to the dashboard name at the top of the page. The text becomes editable. Update the name and click Save.
Create a Dashboard (Classic Interface)

To create a dashboard in the classic interface:

1. In the top navigation bar, click **Dashboards**.

   The **Dashboards** page appears.

2. In the left navigation bar, locate the **Dashboard Templates** folder. You may have to expand the folder if it is closed.

3. Click the dashboard template you want to use to create your own dashboard.

4. Configure the dashboard with the **Dashboard Configuration** and **Component Customization** options.

5. Click **Save**.

   The new dashboard appears in the **My Dashboards** section of the left navigation bar.
Dashboard Settings (Classic Interface)

When creating or updating dashboards, the following options appear.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the dashboard that appears on the left bar.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the contents of the dashboard.</td>
</tr>
<tr>
<td>Target</td>
<td>A drop-down box that contains the options <strong>All Assets</strong> and <strong>Custom</strong>&lt;br&gt;If you select <strong>Custom</strong>, a text box appears where you can enter one or more IP addresses or ranges, separated by commas.</td>
</tr>
</tbody>
</table>
Chart Definitions (Classic Interface)

Each Dashboard is comprised of several different chart types and options. The most common charts are line graph and donut. Line graphs generally provide data over a certain period of time while donut charts provide a percentage or amount out of a set total.

<table>
<thead>
<tr>
<th>Chart</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vulnerabilities Workbench: By Plugin</strong></td>
<td></td>
</tr>
<tr>
<td>Current Vulnerabilities</td>
<td>Each number (Critical, High, Medium, and Low) represents all vulnerabilities discovered within the selected time interval, sorted by severity.</td>
</tr>
<tr>
<td>Vulnerabilities Over Time</td>
<td>Vulnerabilities discovered over time. Each data point on the line graph represents the number of unique vulnerabilities found on a particular day.</td>
</tr>
<tr>
<td>Exploit Available</td>
<td>The number of vulnerabilities tagged as having an exploit available.</td>
</tr>
<tr>
<td>Published Over 30 Days Ago</td>
<td>The number of vulnerabilities first published more than 30 days ago.</td>
</tr>
<tr>
<td>Discovered Using Credentials</td>
<td>The number of vulnerabilities whose plugin_type is &quot;local.&quot;</td>
</tr>
<tr>
<td>Published Solution Available</td>
<td>The number of vulnerabilities that have a remediation available.</td>
</tr>
<tr>
<td>Total Plugins</td>
<td>A list of all the plugins that detected the vulnerabilities that appear on the Vulnerabilities Workbench.</td>
</tr>
<tr>
<td><strong>Vulnerabilities Workbench: By Asset</strong></td>
<td></td>
</tr>
<tr>
<td>Operating System</td>
<td>Displays the operating systems discovered on all scanned assets within the selected time interval.</td>
</tr>
<tr>
<td>Device Types</td>
<td>Displays the device types discovered on all scanned assets within the selected time interval.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Displays the authentication methods discovered on all scanned assets within the selected time interval.</td>
</tr>
<tr>
<td>Chart</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last Scanned</td>
<td>Displays the assets scanned within the selected time interval.</td>
</tr>
<tr>
<td>Assets Over Time</td>
<td>Assets scanned over time. Each data point on the line graph represents the number of unique assets scanned on a particular day.</td>
</tr>
<tr>
<td>Assets Workbench</td>
<td></td>
</tr>
<tr>
<td>All Assets</td>
<td>A list of all scanned assets within the selected time interval.</td>
</tr>
<tr>
<td>Health &amp; Status Workbench</td>
<td></td>
</tr>
<tr>
<td>Current Usage</td>
<td>Each number (<strong>Licensed Assets, Active Agents, Active Scanners</strong>, and <strong>Active Users</strong>) represents the usage and traffic in your instance of Tenable.io.</td>
</tr>
<tr>
<td>Scans Per Day</td>
<td>The number of scans run per day. Each data point on the line graph represents the number of scans run on a particular day.</td>
</tr>
<tr>
<td>Completed Scans</td>
<td>The number of completed scans in Tenable.io. Deleted scans are not included in this number.</td>
</tr>
<tr>
<td>New Scans</td>
<td>The number of new scans in Tenable.io. A scan is considered new if it was created within the last 30 days.</td>
</tr>
<tr>
<td>Scheduled Scans</td>
<td>The number of scheduled scans out of total scans in the system.</td>
</tr>
<tr>
<td>On Demand Scans</td>
<td>The number of on demand scans out of total scans in the system.</td>
</tr>
</tbody>
</table>
Manage Dashboards (Classic Interface)

This section contains the following topics related to managing template-based dashboards:

- Configure a Dashboard
- Configure a Dashboard Component (Classic Interface)
- Set a Default Dashboard
- Filter the Vulnerabilities or Assets Workbench (Classic Interface)
- Delete a Dashboard
- Export a Dashboard
- Advanced Saved Search
- Export a PDF
- Schedule an Export
- Export a Dashboard Image (PNG)
- Modify an Analytics Chart
Configure a Dashboard (Classic Interface)

To configure a dashboard in the classic interface:

1. In the top navigation bar, click **Dashboards**.
2. In the left navigation bar, select the dashboard to be configured.
3. Click the **configure** option.

   The **Configure Dashboard** window will display.

![Configure Dashboard Window](image)

4. The default configuration for **Targets** is set to **Off**.

   Click to toggle the switch on.

   **Note:** The **Targets** option is set to **Off** when the **Dashboard Components** have different configurations. If all of the **Dashboard Components** have the same configuration, the **Targets** option will default to **On**.

5. Select **All Assets**, **Target Group**, or **Custom** to apply configurations to the entire dashboard.

   **Note:** The Dashboard level filters will apply to the entire dashboard. However, changes to individual components can be made using the options on the **Component Customization** page.
6. Make the desired configurations and click **Save**.
7. The newly configured dashboard will display and appear in the My Dashboards section in the left navigation pane.

**Note:** If a template is selected when configuring the dashboard, the newly configured dashboard will be saved as a new dashboard in the **My Dashboards** section in the left navigation pane. If a customized dashboard is configured, the selected dashboard will be saved with the newly configured components.
Configure a Dashboard Component (Classic Interface)

Dashboard components can be easily updated and customized. Use the following steps to configure, reorder, duplicate, and delete components.

**Note:** If a template is selected when customizing a component, the dashboard will be saved as a new dashboard in the My Dashboards section in the left navigation pane. If a customized dashboard component is updated from the My Dashboards section, the selected dashboard will be updated with the new customizations when saved.

To configure a dashboard component in the classic interface:

1. Select the Dashboard component that you want to configure.
2. Hover over the list option.

The available component options will display.

---

### OUTSTANDING REMEDIATIONS BY DEVICE TYPE

<table>
<thead>
<tr>
<th></th>
<th>Assets</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Critical</th>
<th>Exploitable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>55</td>
<td>224</td>
<td>2741</td>
<td>2699</td>
<td>637</td>
<td>32%</td>
</tr>
<tr>
<td>Unix</td>
<td>3</td>
<td>23</td>
<td>156</td>
<td>107</td>
<td>19</td>
<td>8%</td>
</tr>
<tr>
<td>Apple</td>
<td>4</td>
<td>3</td>
<td>27</td>
<td>219</td>
<td>26</td>
<td>57%</td>
</tr>
<tr>
<td>Network</td>
<td>10</td>
<td>1</td>
<td>36</td>
<td>49</td>
<td>8</td>
<td>50%</td>
</tr>
</tbody>
</table>
3. Click the **Configure** option.

A Configure window displays.

4. Make the desired configurations and click **Save**.
To reorder a dashboard component in the classic interface:

1. Select the **Dashboard** that you want to reorder.

2. Click the **Reorder** option.

   The components will move.

3. Drag the components to the desired location.

   **Note:** The easiest way to move a component is to grab the component in the center of the title and drag it to the desired location.

4. Click **Save** to confirm the reordered dashboard.
5. The reordered dashboard is saved.

To duplicate a dashboard component in the classic interface:

1. Select the **Dashboard** component that you want to duplicate.

2. Hover over the list option.

   The available component options will display.
3. Click the **Duplicate** option.

4. A confirmation will display and the duplicated component will be placed after the originally selected component.
To delete a dashboard component in the classic interface:

1. Select the **Dashboard** component that you want to delete.

2. Hover over the list option.

   The available component options will display.
3. Click the **Delete** option.

A confirmation message will appear.
4. Click **Delete** to confirm.

**Delete Component**

Are you sure you want to delete this component?
Deleting components cannot be undone.

[Delete]  [Cancel]

The component is deleted.
Set a Default Dashboard or Workbench (Classic Interface)

The default dashboard acts as the landing page for Tenable.io. You can set any dashboard, including workbenches, as the default dashboard. If you do not set a default dashboard, Tenable.io uses the vulnerabilities workbench as the default.

**Tip:** To navigate back to the default page from another page in Tenable.io, click the Tenable, Inc. logo in the upper left corner of the page.

To set a default dashboard or workbench in the classic interface:

**To the default dashboard from the dashboard screen:**

1. In the top navigation bar, click **Dashboards**.
2. In the left navigation bar, click the dashboard you would like to set as default.
   The selected dashboard appears.
3. Click the **Set as default** option at the top of the screen.

Tenable.io sets the currently displayed dashboard as default.

-or-

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
To set the default dashboard from the left navigation pane:

1. In the left navigation bar, click the ▼ button next to the dashboard that you want to set as default.

2. Click **Set as default**.

Tenable.io sets the selected dashboard as default.
Filter the Vulnerabilities or Assets Workbench (Classic Interface)

To filter the Vulnerabilities or Assets workbench in the classic interface:

1. In the top navigation bar, click **Dashboards**.
   
   The **Dashboards** page appears.

2. In the left navigation bar, click the workbench you want to filter.

3. In the upper right corner, select the **Last 30 Days** drop-down box.

4. Select the interval of time by which you want to filter the data.

   The workbench updates based on your selected filter.

**Note:** You can use the **Advanced** search and search box to further filter the results. Click **Advanced** in the menu bar, and the **Advanced Search** window appears with additional options.

### Advanced Search

- **Match** All of the following:

  - **Asset ID** is equal to **01234567-abcd-ef01-2345-6789**

### Multi-Select Options

Multi-select options are available for **Severity**, **Plugin Family**, and **Target Group** filters. Select the levels of options one at a time from the drop-down box.
Entering Ranges and Multiple Entries

Multiple entries and ranges can be entered for Plugin ID, Hostname, and Port filters. Enter multiple ID's using a comma after each instance. Use a dash to enter ranges. (Multiple entries can also be entered for Plugin Output, Microsoft bulletin, and CVE filters.)
Filter the WAS Workbench (Classic Interface)

**Required Additional License:** Tenable.io Web Application Scanning

**Required Tenable.io Web Application Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To filter the workbench in the classic interface:

1. In the top navigation bar, click the **Dashboards** button.
2. In the left navigation bar, click **Web Applications**.
   - The **Web Applications** workbench appears.
3. In the upper right corner, select the **Last 30 Days** drop-down box.
4. Select the interval of time by which you want to filter the data.
   - The workbench updates based on your selected filter.
Delete a Dashboard (Classic Interface)

To delete a dashboard in the classic interface:

To delete a dashboard from the dashboard screen:

1. In the top navigation bar, click **Dashboards**.

2. In the left navigation bar, click the dashboard you want to delete.

   The selected dashboard appears.

3. Click **Delete**. A window appears, prompting you to confirm your deletion.

4. Click **Delete** to confirm.

   **Delete Dashboard**

   Are you sure you want to delete this dashboard? Once deleted, it cannot be recovered.

   ![Delete Dashboard Window]

Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective owners.
Tenable.io deletes the dashboard. The default dashboard appears.

-or-

To delete a dashboard from the left navigation bar:

1. In the top navigation bar, click Dashboards.
2. In the left navigation bar, click the button next to the dashboard you want to delete.
3. Select Delete from the drop-down menu.

The Delete Dashboard window appears, prompting you to confirm the deletion.

Tenable.io deletes the dashboard. The default dashboard appears.
Export a Workbench (Classic Interface)

This procedure describes exporting a workbench. For information on exporting analytics dashboards, see Export a Custom Dashboard (PDF) (Classic Interface) or Export a Custom Dashboard (PNG) (Classic Interface).

To export a workbench in the classic interface:

1. In the top navigation bar, click **Dashboards**.
2. In the left navigation bar, select the workbench you want to export.
3. (Optional) Filter the workbench data to refine the data for export.
4. In the upper right corner of the page, click the **Export** button.
5. Select one of the following available file formats:

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTML</td>
<td>Web-based HTML file.</td>
</tr>
<tr>
<td>PDF</td>
<td>Adobe PDF file.</td>
</tr>
<tr>
<td>CSV</td>
<td>A comma-separated value (CSV) text file.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Use this format to export workbench data filtered by tag. Tenable.io supports tag filters for this export format only.</td>
</tr>
<tr>
<td>Nessus</td>
<td>Nessus file. Nessus exports are the only file format that can be imported into Tenable.io.</td>
</tr>
</tbody>
</table>

6. Continue as appropriate:
   - If you selected **CSV** or **Nessus**, no further action is required. The file immediately downloads in your browser.
   - If you selected **HTML** or **PDF**, complete the following additional steps:
a. In the **Chapter** drop-down box, select the type of chapters you want to include in the exported dashboard. Options include:

- Current Data
- Executive Summary
- Differential Report

b. Click **Export**.

The file immediately downloads in your browser.
Export a Custom Dashboard (PNG) (Classic Interface)

You can use the **Export** option to share a screenshot of a customized dashboard.

To configure a custom dashboard as a PNG file in the classic interface:

1. In the top navigation bar, click **Dashboards**.
2. In the left navigation bar, select the **Analytics Dashboard** that you want to export.
   
   **Note:** The exported image only contains the information currently displayed on the screen. Make sure the desired sections are visible on the screen before you begin the export.
3. Click the 🖼️ button at the top of the page.
4. Select **PNG** from the drop-down list.

   The export begins. A loading icon appears as the system processes the export.

   **Note:** Dashboards that contain pie charts may take longer to export.

Once processing completes, the button with the exported file appears at the bottom of the page:
5. Click the button at the bottom of the page to open the file.

The exported dashboard file appears. See the table below for sample outputs.

<table>
<thead>
<tr>
<th>Dashboard Type</th>
<th>Export Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploitable by Malware</td>
<td></td>
</tr>
</tbody>
</table>
Exploitable by Malware

Outstanding Remediation Tracking
Vulnerability Management
Export a Custom Dashboard (PDF) (Classic Interface)

You can use the Export PDF feature to share customized dashboards externally (for example, in email and presentations). The exported PDF is a generated report of the selected dashboard.

To configure a custom dashboard as a PDF file in the classic interface:

1. In the top navigation bar, click Dashboards.
2. In the left navigation bar, select the Analytics Dashboard that you want to export.
3. Click the button at the top of the page.
4. Select Export PDF from the drop-down list.

A processing icon appears as the PDF is generated. Once generated, the PDF downloads to your system. The displayed output varies depending on the web browser you are using.

Note: You can also export a PDF using the Schedule Export option. This option provides a variety of settings to schedule a PDF report of the selected dashboard.
Schedule a Custom Dashboard Export (Classic Interface)

You can use the **Schedule Export** option to schedule times to send PDF exports of customized dashboard views to specified recipients. The exported PDF is a generated report of the selected dashboard.

**Note:** Tenable.io does not support report attachments larger than 18MB.

To schedule an export of a custom dashboard in the classic interface:

1. In the top navigation bar, click **Dashboards**.
2. In the left navigation bar, select the **Analytics Dashboard** you want to export.
3. Click the 🕒 button at the top of the page.
4. In the drop-down menu, select **Schedule Export**.
   
   The **Schedule Export** window appears.

5. Configure the settings for the scheduled export:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recipients</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Address</td>
<td>(none)</td>
<td>Enter the email address or addresses you want to receive the export report.</td>
</tr>
<tr>
<td><strong>Export Schedule</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frequency</td>
<td>Once</td>
<td>Specifies how often the scan launches.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Once</strong>: Schedule the scan at a specific time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Daily</strong>: Schedule the scan to occur on a daily basis, at a specific time or to repeat up to every 20 days.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Weekly</strong>: Schedule the scan to occur on a recurring basis, by time and day of week, for up to 20</td>
</tr>
</tbody>
</table>
• **Monthly**: Schedule the scan to occur every month, by time and day or week of month, for up to 20 months.

• **Yearly**: Schedule the scan to occur every year, by time and day, for up to 20 years.

| Starts   | Varies | Specifies the exact date and time when a scan launches. The starting date defaults to the current date. The starting time is the nearest half-hour interval. For example, if you create your scan on 10/31/2016 at 9:12 AM, the starting date and time defaults to 10/31/2016 and 09:30. |
| Time Zone | Varies | Specifies the timezone of the value set for **Starts**. |
| Repeat Every | Varies | Specifies the interval at which Tenable.io relaunches a scan. The default value of this item varies based on the frequency you choose. |
| Repeat On | Varies | Specifies what day of the week a scan repeats. This item appears only if you specify **Weekly** for **Frequency**. The value for **Repeat On** defaults to the day of the week on which you create the scan. |
| Repeat By | Day of the Month | Specifies when Tenable.io relaunches a monthly scan. This item appears only if you specify **Monthly** for **Frequency**. |
| Summary | Not Applicable | Provides a summary of the schedule for your scan based on the values you specified for the available |
| Encrypt PDF | Off | When the Encrypt PDF option is set to On, the Encryption Password box appears. Enter a password to complete the encryption configuration. |

6. **Click Schedule Export.**

A processing icon appears as the system saves the information.

Once the save is complete, a confirmation message appears at the top of the screen. The export is sent according to the set schedule.

**Note:** If you use a Dashboard Template when scheduling an export, two confirmation messages appear. One confirms the scheduled export. The other confirms the addition of a copy of the template to the My Dashboards section.

**Note:** After you schedule an export, the Scheduled Export option appears at the top of the dashboard. Occasionally, you may have to refresh the browser page for this option to appear.

To view a summary of the schedule information, hover over the Scheduled Export option. To modify the export schedule, click the Schedule Export option, then modify the settings in the Schedule Export window.
Advanced Saved Search (Classic Interface)

You can use the Advanced Saved Search to save frequently searched parameters and share them with other team members.

**Note:** Saved searches are available on the vulnerabilities workbench, assets workbench, and Scans page.

Create a Saved Search

To create a saved search in the classic interface:

1. Click the Advanced option in the top navigation bar.

   A new window appears.

2. Select the filter options.
3. Click the **save** button.

A **Name** field appears.

4. Enter a name for the search and click **Save**.
5. A confirmation appears at the top of the screen. If this is the first saved search, a **Saved** option appears next to the **Advanced** option in the top navigation bar. All saved searches are listed under the **Saved** option.

![Advanced Search](image)

**Note:** Names can consist of alphanumeric and special characters.
**Note:** If you click **Apply**, the filter is temporarily saved. When the filter is temporarily saved, a notification appears in the top navigation bar. Click the notification to open, name, and permanently save the filter.

**Note:** Saved searches are context driven and dynamically update based on your current location within Tenable.io, i.e., saved searches created in the Vulnerabilities Workbench are only available when viewing the Vulnerabilities Workbench page and cannot be viewed when on the Scans or Assets page.

### Edit Search Name

To edit the saved search name in the classic interface:

1. To update the name, click the edit button next to the title.

2. Click the **confirm** button to confirm the name update.

   A confirmation message appears at the top of the screen, confirming the name has been saved.
Add a New Filter

To add a new filter to the saved search in the classic interface:

1. Click the **Advanced** option and select the saved search to be edited from the drop down list.

   The selected search appears with the existing filters.

2. Click the **add** button next to the currently set filter.

   A new row of filter options appears.
3. Enter the filter information.

A message appears, prompting you to confirm the update.

4. Click **Update** to confirm the change.

The window closes, and a confirmation message temporarily appears at the top of the screen.

**Remove a Filter**

To remove a filter from the saved search in the classic interface:
1. Click the **Advanced** option and select the saved search to be edited from the drop down list.

   The selected search appears with the existing filters.

   ![Advanced Search](image1)

2. Click the **Delete** button next to the filter to be removed.

   A message appears, prompting you to confirm the update.

   ![Severity Search](image2)
3. Click **Delete** to confirm the change.

![](image)

4. The window closes, and a confirmation message temporarily appears at the top of the screen.

**Delete a Saved Search**

To delete a saved search in the classic interface:

1. Click the **Advanced** option
   
   The selected search appears with the existing filters.

2. Select the saved search you want to delete.
3. Click the **Delete** button at the top of the new window.

A confirmation message appears at the top of the window to confirm the removal of the search.

4. Click **Delete** to complete the deletion.

**Caution:** Deletions cannot be undone.

**Share a Saved Search**

To share a saved search in the classic interface:
1. Click the **Advanced** option and select the saved search to be shared from the drop down list.

   The selected search appears with the existing filters.

   ![Advanced Search](image1)

2. Click the **share** button.

   An option to select users and user groups appears.

   ![Severity Search II](image2)

3. Type the user name or select it from the drop-down box.
4. Click **Send Saved Search**.

A confirmation message appears.

**Note:** The shared search appears in the user's list of saved searches.

**Viewing Options**

Users can view the saved searches using two methods.

To view a saved search in the classic interface:
1. Click the **Advanced** option.

2. Select the saved search from the drop down menu

-or-

1. Click the **Saved** option.

2. Select the saved search from the list.

3. Click the **Advanced** option.

   The selected saved search appears.

**Note:** When a search is selected, a number appears next to the **Advanced** option. This number represents the number of filters in the selected search.

Indicates the number of filters in the selected saved search.
Modify a Custom Dashboard Chart (Classic Interface)

To modify a chart in a custom dashboard in the classic interface:

1. In the top navigation bar, click **Dashboards**.
2. In the left navigation bar, click the analytics dashboard that contains the chart that you want to modify.
3. For the chart that you want to modify, click the pencil button.
4. Modify the settings as needed.
5. Click **Save**.

Tenable.io updates the chart.
Reports (Classic Interface)

Reports can be considered in two parts: the report definitions, and the results. Using the Reports page, you can create a report and configure its definitions, run existing reports, and view the results of those reports. To access the Reports page, on the top navigation bar, click Reports.

Note: PCI Quarterly External scan data is intentionally excluded from dashboards, reports, and workbenches. This is due to the scan's paranoid nature, which may lead to false positives that would otherwise not be detected. For more information, see PCI ASV Scanning Overview.

The Reports page includes the following folders:

- The My Reports folder is the default folder that appears when you access the Reports page. Reports that you create will appear in this folder.

- The All Reports folder displays all reports that you have permission to interact with. If you are using an administrator account, then this folder will display all reports that have been created by your organization.

- The All Report Results folder displays all of the results from reports that you have permissions to view. If you are using an administrator account, then this folder will display all results from reports that are created by your organization. Results are displayed in chronological order based on when the reports were run.

- The Trash folder displays report definitions (i.e., the reports that appear in the My Reports and All Reports folders) that are deleted. In the Trash folder, you can restore deleted reports or permanently delete them.

Using Tenable.io, you can generate thematic, informative reports to help you find information that might otherwise be overlooked. For example, the Credentialed Scan Failures report delivers a straightforward, organized list of failed credentialed scans that analysts can use to quickly address scanning issues, making it simpler to troubleshoot problems with credentialed scans. This documentation includes a complete list of report templates included with Tenable.io.

Reports can be run on demand or scheduled to run periodically, providing a regular view of the state of various facets of your assets. Additionally, you can specify individuals and groups that have access to the reports. Permissions range between a user being limited to viewing report results to a user being able to fully configure and run that report. For more information about scheduling, permissions, and other information regarding configuring reports, see Report Settings.
If this is your first time using the Reports feature, see the Reports Workflow, which provides a basic explanation of the steps you can take to start leveraging reports.
Reports Workflow (Classic Interface)

The following workflow is intended as a basic guide for getting started with the Reports feature of Tenable.io for the first time. It is not a best practice, and may not correspond to the requirements of your organization.

1. As an organization, review the report templates provided in Tenable.io, and identify reports that are relevant to the requirements of your organization.

2. As an organization, identify appropriate schedules for the reports that you want to run.

3. Create the relevant reports and schedule them based on the requirements identified by your organization.

4. Run on-demand reports as needed.

5. Review the results of the reports. Based on the results, identify actions that are required by members of your organization. Additionally, identify if new reports are now required.

6. Periodically review the requirements of your organization. Create or modify reports if the requirements have changed, and delete reports that are obsolete.
Report Settings (Classic Interface)

When you create a new report or modify an existing report, the following options are available:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>This text box displays the name of the report template you selected. You can edit this text box to rename the report.</td>
</tr>
<tr>
<td>Description</td>
<td>This text box displays a default description based on the report template you selected. You can edit this text box to modify the description of the report.</td>
</tr>
<tr>
<td><strong>Target</strong></td>
<td>This drop-down box includes the following values:</td>
</tr>
<tr>
<td></td>
<td>• <strong>All Assets</strong>: The report will target all assets that you have permission to scan. If you are using an administrator account, the report will target all of your organization's assets.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Target Groups</strong>: The report will target a specified group of assets. When you select this option, a drop-down box appears that includes all of the groups that you have permission to access. If you are using an administrator account, all groups created by your organization will be available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Custom</strong>: The report will target a comma-delimited list of IP addresses, CIDR notation, and hostnames. When you select this option, a text box appears. The list of targets must be specified in that box.</td>
</tr>
<tr>
<td></td>
<td>By default, a report will target all available assets.</td>
</tr>
<tr>
<td>Encrypt PDF</td>
<td>By default, PDFs created by a report are not encrypted. When the <strong>Encrypt PDF</strong> option is set to <strong>On</strong>, the <strong>Encryption Password</strong> box appears.</td>
</tr>
<tr>
<td>Encryption Password</td>
<td>This text box is used to specify a password for encrypted PDFs created by the report. It is only visible when the <strong>Encrypt PDF</strong> option is set to <strong>On</strong>.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Email</td>
<td>This text box provides the option to include email addresses for recipients.</td>
</tr>
<tr>
<td><strong>Schedule</strong></td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>By default, reports are configured to be run on demand. When the <strong>Enabled</strong> option is set to <strong>On</strong>, the <strong>Frequency</strong>, <strong>Starts</strong>, and <strong>Timezone</strong> options appear. Additionally, a summary of the specified schedule appears following the other options. The summary updates as you make changes to the other options.</td>
</tr>
<tr>
<td><strong>Frequency</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A drop-down box that includes the following values:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Once</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Daily</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Weekly</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Monthly</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Yearly</strong></td>
</tr>
<tr>
<td></td>
<td>By default, this option is set to <strong>Once</strong>.</td>
</tr>
<tr>
<td><strong>Starts</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A text box and a drop-down box used to select or type a date and time when the report will run.</td>
</tr>
<tr>
<td><strong>Timezone</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A drop-down box used to select or type a time zone.</td>
</tr>
<tr>
<td><strong>Permissions</strong></td>
<td></td>
</tr>
<tr>
<td><strong>User Sharing</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the <strong>User Sharing</strong> section, you specify users or groups that you want to give access to the report and its results. Users and groups appear in rows at the bottom of the section.</td>
</tr>
<tr>
<td></td>
<td>The following permissions can be specified:</td>
</tr>
<tr>
<td></td>
<td>• <strong>No access</strong>: This user or group cannot access the report or its results in any way.</td>
</tr>
</tbody>
</table>
### Option Description

- **Can view**: This user or group can see when the report is running and download the results.

- **Can control**: This user or group can run the report in addition to viewing it.

- **Can configure**: This user or group can configure the report in addition to running and viewing it. If a user has permission to configure a report created by someone else, the assets and groups that are available as targets will be those that *the owner* has access to. Because of this, groups that the *configuring user* does not normally have access to may appear in the **Targets** drop-down box.

**Note:** Users with administrator accounts always have full control over a report as though they owned it.

Permissions are considered using this hierarchy: **Default > Group > User**. Permissions that are assigned to a specific group always supersede the permissions specified for the **Default** group. Permissions that are assigned to a specific user always supersede the permissions specified for any group that user belongs to.

**Note:** Permissions are not applied retroactively. For example, if a report runs on the 15th of each month of 2021 and a user is given permission for that report on April 1 (before the report is run that month), that user will not have access to the results for January, February, and March.

By default, all reports include the following:

- The user who created the report, set to **Is owner**. This value cannot be changed.

- The **Default** group, which represents all of your organization’s Tenable.io users. When you create the report, the **Default** group is set to **No Access**. Other users will not be able to access, run, configure, or see the results of the report.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neither the owner of the report nor the Default group can be removed from the User Sharing section.</td>
<td></td>
</tr>
</tbody>
</table>

In the Add users or groups text box, type the name of the user or group that you want to specify a permission for. The text box searches for users and groups as you type. After you select a user or group, the name is added as a row at the bottom of the section and a drop-down box appears beside the name that you use to specify the desired permission.

For example, you create a report. The permission for the Default group is set to No access. Suppose you have a group called Risk Analysts. For your report, you set the permission for the Risk Analysts group to Can control. Mary is the manager of the risk analysis team, and a member of the Risk Analysts group. For your report, you set the permission for Mary to Can configure so she can modify the report for her team as necessary. The report now prevents any users beyond you (the owner) and the Risk Analyst group from interacting with the report. Team members that belong to the Risk Analysts group can run the report as needed. If for some reason the report needs to be modified, the team members can request those modifications through their manager, Mary, who has permission to configure the report.

Chapters

**Chapters** displays the arrangement of the chapters, groups, paragraphs, and other components that appear in the results of the report. You can expand and view the arrangement. It cannot be modified.
Report Templates (Classic Interface)

The following templates are included with Tenable.io:

- CVE Analysis Report
- Credentialed Scan Failures
- Critical and Exploitable Vulnerabilities Report
- Elevated Privilege Failures
- Exploit Frameworks
- Exploitable by Malware
- Malicious Code Prevention Report
- Outstanding Patch Tracking
- Prioritize Hosts
- Unsupported OS Report
- Vulnerabilities by Common Ports
- Vulnerability Detail Report
- Vulnerability Management
- Web Services Indicator
- Windows Unsupported and Unauthorized Software
- Wireless Configuration Report

The following table lists the report templates that are included with Tenable.io and the complete descriptions that are provided for each.

<table>
<thead>
<tr>
<th>Report Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE Analysis Report</td>
<td>In the early days of the internet, vulnerabilities were not publicly known or identifiable. In 1999, the information security industry endorsed the import-</td>
</tr>
<tr>
<td>Report Template</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>The adoption of CVE has grown from 29 organizations to over 150 organizations. Tenable products were first CVE compatible in 2004. Tenable continues to lead the security industry in vulnerability management and continuous network monitoring by embracing accepted standards such as CVE. CVE identifiers are used to reference each of the vulnerabilities detected by Tenable Nessus. The CVE identifiers can be used for reporting, asset identification, risk management, and threat mitigation. This report helps to identify vulnerabilities by their CVE identifiers from 1999 to 2019. CVE is a widely used industry standard for identifying vulnerabilities across software vendors and vulnerability management systems. Using CVE identifiers to identify vulnerabilities allows organizations to easily target affected systems and software for remediation. As vendors provide patches for widespread vulnerabilities such as HeartBleed and ShellShock, many new plugins are released. The task of tracking vulnerabilities is simplified by using CVE identifiers, as the CVE identifiers for vulnerabilities remain the same even as new patches and plugins are released. Using CVE is a very flexible and useful method of detecting vulnerabilities to assist in the risk management process. This report provides an easy to understand executive summary showing the current count of vulnerabilities based on CVE release data and collection methods. The remaining chapters provide details on the top 100 most severe CVE vulnerabilities.</td>
</tr>
<tr>
<td>Credentialed Scan Failures</td>
<td>Scanning without credentials is a valid method for identifying what is visible to the scanner and assessing the exterior attack surface of a system, but properly configured credentialed scans are able to look beyond the surface and identify potential issues that may not be apparent. Credentialed scans provide more detailed results that can help to detect outdated software, vulnerabilities, and compliance issues. Without proper credentials, analysts will not be able to obtain accurate information to properly assist...</td>
</tr>
<tr>
<td>Report Template</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>an organization’s risk posture.</td>
<td>This report delivers an organized list of failed credentialed scans that analysts can use to quickly address scanning issues on a network. The report covers a 25-day scanning history and provides a breakdown of various Windows scan issues and SSH failures, as well as general credential failures. Organizations will find this report useful when reviewed on a daily or weekly basis. The report is organized in a manner that provides timely information that analysts can use to correct any credentialed scan failures.</td>
</tr>
<tr>
<td>Critical and Exploitable Vulnerabilities Report</td>
<td>Identifying, prioritizing, and patching existing vulnerabilities on a network can be a difficult task for any analyst to manage effectively. By determining which vulnerabilities are most severe, analysts can properly prioritize vulnerability remediation in order to best protect systems on the network. This report presents a comprehensive look at the critical and exploitable vulnerabilities discovered on the network, which can be useful in reducing the overall attack surface and keeping critical data secured within an organization. Tenable products collect a vast amount of data on existing vulnerabilities discovered on the organization's network. Detailed analysis and understanding of risk for each vulnerability can be time consuming. However, the analyst should at least understand the impact of each vulnerability in order to understand the threat posed. The severity of a vulnerability is defined using the Common Vulnerability Scoring System (CVSS) base score. The CVSS is a method to define and characterize the severity of a vulnerability. Vulnerabilities are scored on a scale of 1 to 10, with a CVSS base score of 10 considered to be the most severe. Vulnerabilities with a CVSS base score of 10 are defined as &quot;critical.&quot; In addition to specifying the severity of a vulnerability, industry sources are checked to determine if a publically-known exploit for the vulnerability exists. These critical and exploitable vulnerabilities create gaps in the network's integrity, which attackers can take advantage of to gain access to the network. Once</td>
</tr>
<tr>
<td>Report Template</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>inside the network, an attacker can perform malicious attacks, steal sensitive data, and cause significant damage to critical systems. By identifying the most severe vulnerabilities, analysts and security teams can better focus patch management efforts and better protect the network. This report provides information on critical and exploitable vulnerabilities that have been detected on the network. The report utilizes data such as the CVSS base score and information from exploit frameworks including Metasploit, Core Impact, Canvas, Elliot, and ExploitHub to determine which vulnerabilities are critical and exploitable. The report presents a cumulative view of the data to provide an analyst with a comprehensive understanding of the discovered critical and exploitable vulnerabilities. Using various visual aids, the report displays the data in an easy to understand manner. The information from this report will enable analysts to discover, prioritize, and remediate critical and exploitable vulnerabilities in a timely manner.</td>
</tr>
<tr>
<td>Elevated Privilege Failures</td>
<td>Organizations using Tenable Nessus gain a tremendous amount of details such as vulnerabilities, compliance status, software used, and hardware supporting the environment. Nessus provides valuable insight into systems to an analyst, to enable better protection of the network. As with any piece of software or hardware, Nessus needs to be properly configured to ensure the best scan results are returned. For scans of Linux/Unix based systems, analysts can configure the scans to use SSH username/password credentials, which allows Nessus to gather more detailed information about the systems. If a Nessus scan is configured with SSH credentials for a regular user account, basic information about a system can be retrieved. Once Nessus is able to create a session with SSH, Nessus will try to elevate privileges to retrieve further information about the system. If Nessus is unable to perform this action, Nessus plugin 12634 will report that the attempt to elevate permissions was unsuccessful (see <a href="https://community.tenable.com/message/14694">https://community.tenable.com/message/14694</a>). Using this report, analysts can identify systems that did not have adequate permissions to do in-</td>
</tr>
<tr>
<td>Report Template</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>depth scanning. Details are also provided to assist analysts in remediating the SSH credential issue. To prevent confusion, this report only addresses failures when Nessus attempts to elevate privileges from a scan; this report does not address attempts by users who try to elevate privileges and are unsuccessful.</td>
<td>Organizations of all size are faced with the challenges of maintaining a successful patch management program. In many cases, vulnerability scans and software updates are only performed on a monthly basis. The lack of visibility into the network and systems in between active scans can result in an increased risk to the organization. This point-in-time method of scanning and updating can also lead to systems being missed if the systems are not on the network or available during the scan window. A single vulnerability is often times the only necessary piece needed to gain a foothold in an environment. As an example, a network could be compromised due to a vulnerability found in out-of-date office productivity software, a PDF viewer, or a browser. Exploitation framework tools contain capabilities to detect and exploit these vulnerabilities. The vendors of these software packages are continually adding exploits to their platforms. Internal security teams and malicious actors alike can use the same tools to detect and exploit vulnerabilities. As some of the software exploitation tools are free, the bar of entry is minimal and can open up organizations to easy to perform attacks. This report can assist analysts in identifying vulnerabilities detected within the organization. Specifically, the report detects vulnerabilities that can be exploited by exploitation frameworks. Analysts can focus on the exploitable vulnerabilities to help reduce the risk to the organization. These specific exploitable vulnerabilities can present a heightened risk depending on the vulnerability and location in the organization. Analysts using this report can be more efficient at prioritizing efforts by knowing more about the vulnerabilities present in the organization. Within this report, analysts can find detailed information relating to the vulnerabilities exploitable by exploitation frameworks. The detailed...</td>
</tr>
<tr>
<td>Report Template</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>information includes the host, vulnerability, and related information for each exploitation tool. There are also tables reporting vulnerabilities by plugin family, Microsoft bulletins, and CVE. Depending on the reporting metrics used within the organization, analysts can potentially compare the information from this report to their metrics for quick analysis. Information is also provided to assist analysts and administrators in fixing and mitigating the vulnerabilities.</td>
</tr>
<tr>
<td>Exploitable by Malware</td>
<td>Malware presents a risk to any organization and comes packaged in many forms. Malware can exploit weaknesses and vulnerabilities to make software or hardware perform actions not originally intended. Vulnerabilities can also be widely exploited shortly after publication as malware authors reverse engineer the fix and come up with &quot;1-day exploits&quot; that can be used to attack organizations. Using this report, organizations can gain operational awareness of systems on the network with exploitable vulnerabilities. Analysts need to either mitigate the risk from vulnerabilities or remediate them, but prioritization is a necessary task, as not all vulnerabilities present an equal danger. Focusing on vulnerabilities actively exploited by malware helps to reduce the risk to the organization and offers prioritization guidance as to which vulnerabilities to remediate first. Analysts can use this report along with the knowledge of the software in the organization to better defend themselves. Vulnerabilities can also be exploited through common software applications. An attacker can use these software products to exploit vulnerabilities present in an organization. Products such as Metasploit, Core Impact, and exploits listed in ExploitHub can be used by anyone to perform an attack against vulnerabilities. Vulnerabilities that can be exploited through these means are highlighted in this report.</td>
</tr>
<tr>
<td>Malicious Code Prevention Report</td>
<td>Malware can significantly impact the health and safety of critical systems within an organization. The number of new malware discovered on a daily basis continues to increase, and malware writers are constantly tweaking</td>
</tr>
<tr>
<td>Report Template</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>their code to keep it from being detected. Using malicious code, potentially massive attacks can be accomplished with relative ease. Network defenders need to use a defense-in-depth approach to both protect against malware infections and also discover and address any malware that gets through defenses. Inside this report, analysts will obtain the information needed to identify compromised hosts that have been infected with malware. Additional information on virus detections and interactions with known hostile IP addresses will highlight the presence of malware on network assets. Scans will determine whether anti-virus engines and virus definitions are running and up-to-date. Analysts will be able to obtain information on outdated or misconfigured anti-virus clients on the network. Systems are scanned for bad AutoRuns and Scheduled Tasks that may be associated with malware. Using the information presented within this report, organizations are able to quickly identify and remediate issues associated with malware or malicious activity on systems throughout the enterprise.</td>
</tr>
</tbody>
</table>

| Outstanding Patch Tracking | One of the common questions often asked of the IT team is "how many systems are missing patches and how many patches are missing on each system?" This report uses the Tenable Nessus "Patch Report" plugin (66334) and organizes the current patch status for systems scanned with credentials. The IT team can now easily communicate the specific systems with missing patches to executives. The "Patch Report" plugin elegantly summarizes all of the missing patches and general remediation actions required to remediate the discovered vulnerabilities on a given host. Instead of counting the number of vulnerabilities, the plugin lists applications that need to be upgraded. The approach is not only much easier for IT administrators to consume, but the count of applications provides a measure of how much "work" is required to secure a system. In addition, this report can help analysts monitor the application of Microsoft Security Bulletin patches. The elements of this report displays information on missing Microsoft Security Bulletin patches, in order to provide a clear
<table>
<thead>
<tr>
<th>Report Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prioritize Hosts</td>
<td>What systems need attention now? What systems can be safely ignored for the time being? System administrators often have so much to do that it can be difficult for them to prioritize their host administration and mitigation efforts. This report can assist in that prioritization by presenting multiple lists of top hosts in various categories, such as top hosts infected with malware and top hosts with exploitable vulnerabilities. The elements in this report make use of active scan information from Tenable Nessus. In this way, a system administrator can obtain the most comprehensive and integrated view of the network, in order to make the best prioritization decisions about administration and mitigation efforts.</td>
</tr>
<tr>
<td>Unsupported OS Report</td>
<td>Detecting unsupported operating systems on a network can be a daunting task. Understanding which operating systems are unsupported or approaching end-of-life (EOL) can improve a security team's ability to mitigate vulnerabilities and secure the network. Systems running unsupported operating systems are more vulnerable to exploitation, so identifying and upgrading unsupported operating systems on a network is essential to an effective security program. Using this report, security teams can easily identify and address unsupported operating systems on a network. The chapters in this report provide detailed information about the unsupported operating systems detected by Nessus on the network. Elements filter by plugin name and vulnerability text in order to provide the most accurate overview of unsupported operating systems. A list of detailed information provides insight into systems running unsupported operating systems and recommended steps to address the vulnerabilities. Security teams can use the data in this report to detect and upgrade unsupported operating systems.</td>
</tr>
<tr>
<td>Vulnerabilities by Common Ports</td>
<td>Addressing vulnerable services is a key step in reducing network risk. Vulnerable services may allow malicious actors to infiltrate the network, compromise systems, and exfiltrate information. This report presents</td>
</tr>
</tbody>
</table>

Report Template | Description
--- | ---
picture of the true state of Microsoft patch management.
Prioritize Hosts | What systems need attention now? What systems can be safely ignored for the time being? System administrators often have so much to do that it can be difficult for them to prioritize their host administration and mitigation efforts. This report can assist in that prioritization by presenting multiple lists of top hosts in various categories, such as top hosts infected with malware and top hosts with exploitable vulnerabilities. The elements in this report make use of active scan information from Tenable Nessus. In this way, a system administrator can obtain the most comprehensive and integrated view of the network, in order to make the best prioritization decisions about administration and mitigation efforts.
Unsupported OS Report | Detecting unsupported operating systems on a network can be a daunting task. Understanding which operating systems are unsupported or approaching end-of-life (EOL) can improve a security team's ability to mitigate vulnerabilities and secure the network. Systems running unsupported operating systems are more vulnerable to exploitation, so identifying and upgrading unsupported operating systems on a network is essential to an effective security program. Using this report, security teams can easily identify and address unsupported operating systems on a network. The chapters in this report provide detailed information about the unsupported operating systems detected by Nessus on the network. Elements filter by plugin name and vulnerability text in order to provide the most accurate overview of unsupported operating systems. A list of detailed information provides insight into systems running unsupported operating systems and recommended steps to address the vulnerabilities. Security teams can use the data in this report to detect and upgrade unsupported operating systems.
Vulnerabilities by Common Ports | Addressing vulnerable services is a key step in reducing network risk. Vulnerable services may allow malicious actors to infiltrate the network, compromise systems, and exfiltrate information. This report presents
<table>
<thead>
<tr>
<th>Report Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vulnerability information by common TCP ports and services, in order to alert the analyst to potentially vulnerable services. The elements in this report leverage a variety of active and passive port filters to display vulnerability information in multiple ways. System counts and vulnerability counts are presented based on specific ports, ranges of ports, and CVSS scores. Vulnerabilities that are known to be exploitable are highlighted; these vulnerabilities are especially concerning and should be addressed immediately. The vulnerability information in this report can be used to remediate service vulnerabilities and improve the security of the network.</td>
</tr>
<tr>
<td>Vulnerability Detail Report</td>
<td>Vulnerability scanning and reporting are essential steps in evaluating and improving the security of a network. By knowing which vulnerabilities affect hosts on the network, security teams can coordinate their mitigation efforts more effectively. Nessus provides this vulnerability scan information. This report presents extensive data about vulnerabilities detected on the network. The report can be especially useful to security teams that are familiar with the format and content of reports generated by Nessus. Detailed information about the vulnerabilities detected on every host scanned is included. Security teams can use this report to easily identify vulnerabilities and the affected hosts in their network. The chapters in this report provide both a high-level overview and an in-depth analysis of the vulnerability status of the network. Charts are used to illustrate the ratio of vulnerability severities as well as list the most vulnerable hosts by vulnerability score. An iterator is used to provide detailed information on each host scanned. For each host, the IP address, DNS name, NetBIOS name, MAC address, repository, vulnerability total, and last scanned time are listed. A severity summary of each host shows how many vulnerabilities of each severity level impact that host. Detailed information about every vulnerability detected on that host is listed, including plugin ID, plugin name, plugin family, severity, protocol, port, exploitability, host CPE, plugin text, first discovered, and last seen times. Security teams can use this extensive data in order to identify vulnerabilities in their network and tailor their</td>
</tr>
<tr>
<td>Report Template</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>Vulnerable devices and applications on an organization's network pose a great risk to the organization. Vulnerabilities such as outdated software, susceptibility to buffer overflows, risky enabled services, etc. are weaknesses in the network that could be exploited. Organizations that do not continuously look for vulnerabilities and proactively address discovered flaws are very likely to have their network compromised and their data stolen or destroyed. This report provides a high-level overview of an organization's vulnerability management program and can assist the organization in identifying vulnerabilities, prioritizing remediations, and tracking remediation progress. In addition, this report assists in monitoring for sensitive data and data access vulnerabilities on the network. By understanding where sensitive or valuable information is kept and any associated vulnerabilities, security teams can better ensure file security and integrity.</td>
</tr>
<tr>
<td>Web Services Indicator</td>
<td>Services across enterprises are increasingly becoming web connected, but not all web services are secure. Organizations need to know what web services are operating in the environment in order to understand their vulnerability status. This report provides insight into the web services in the environment and the vulnerabilities associated with them. Administrators and analysts can better assess and defend the organization when they have the necessary information. This report provides information based around web services in the environment. Web services and the technology that hosts them are supported and implemented in various ways. The vulnerabilities of web services, web service platforms, and related technologies are displayed in ways that are easy to understand. Analysts can see vulnerabilities based on ports, web service activities leaving the organization, and web services that are present with known vulnerabilities. Network defenders can use the insight into the vulnerabilities in web services provided by this report to more effectively secure their network.</td>
</tr>
<tr>
<td>Report Template</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Windows Unsupported and Unauthorized Software</td>
<td>The proliferation of unsupported products is an issue for many organizations and increases the effort required to minimize risk. As applications reach their end-of-life (EOL), vendors stop offering support. As patches and updates are released for new versions of software, unsupported versions will be left out. Essentially zero-day vulnerabilities could be in effect for applications that are no longer supported. Therefore, security and stability decrease, raising concern as time progresses. Identifying systems running unsupported applications is an important part of assessing and minimizing organizational risk. This report presents unsupported and unauthorized products found in the environment. Elements include pie charts and tables to display, track, and report on unsupported and unauthorized applications. Vulnerability data for unsupported vulnerabilities is filtered using Nessus plugin 20811, Microsoft Windows Installed Software Enumeration, as well additional filters for unsupported applications. Within this report, sections include Wireshark, WinPcap, TeamViewer, and Steam as examples of unauthorized applications.</td>
</tr>
<tr>
<td>Wireless Configuration Report</td>
<td>As organizations continue to evolve, wireless technologies are being integrated into existing networks to support employee mobility needs. Since wireless access can expose devices to unique threats, monitoring devices for access to suspicious or malicious wireless networks is essential. This report provides extensive information about the wireless networks accessed by scanned hosts in the organization. Several specific plugins are used to gather extensive details about wireless interfaces and SSID connections from Windows and macOS hosts. Security teams can use this report to easily examine wireless configuration details for scanned hosts and tailor scanning policies in order to include additional hosts. The chapters in this report present both a high-level overview and an in-depth analysis of the wireless configurations detected on hosts in the network. Charts and tables demonstrate which plugins were able to successfully gather wireless configuration details from scanned hosts. An iterator is used to provide extensive detail about wireless configurations of each...</td>
</tr>
<tr>
<td>Report Template</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>host, including network interfaces and SSID histories. Security teams can use this detailed report to identify and monitor the wireless connections and configurations of hosts in the organization.</td>
</tr>
</tbody>
</table>
Manage Reports (Classic Interface)

This section contains the following topics related to managing reports:

- Create a New Report
- Modify an Existing Report
- Run a Report
- View Report Results
- Delete a Report
- Recover a Report
- Delete Report Results
Create a New Report (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

To create a new report:

1. On the top navigation bar, click **Reports**.
   
   The **Reports** page appears.

2. In the upper right corner, click the **New Report** button.
   
   The **Report Templates** section appears, displaying a list of the available report templates.

3. Select a template from the list.
   
   The **New Report** section appears and the **General** settings tab is active.
4. Configure the **General settings:**
   
a. In the **Targets** box, select a target for the report. By default, the **Target** box is set to **All Assets**.
   
b. (Optional) Set the **Encrypt PDF** option to **On** and specify a password for the PDF.
   
c. (Optional) In the **Name** box, specify a name for the report.
   
d. (Optional) In the **Description** box, modify or replace the default report description.
   
e. (Optional) In the **Email** box, enter the email addresses for report recipients.

5. (Optional) Configure the **Schedule settings:**
   
a. In the **Settings** section, under **BASIC**, click **Schedule**.

   The **Schedule** settings appear.
b. Set **Enabled** to **On**, and then specify the desired frequency, start time and date, and timezone.

6. (Optional) Configure the **Permissions** settings:

   **Note:** If you do not configure the **Permissions** settings, only you and users with administrator accounts will have access to the report and its results.

   a. In the **Settings** section, under **BASIC**, click **Permissions**.

      The **Permissions** settings appear.

   b. In the **Add users or groups** box, type the name of the user or group that you want to give permissions for the report.
The specified user or group appears in a row at the bottom of the **User Sharing** section.

c. In the row corresponding to the user or group that you added, in the drop-down box, select a permission.

7. *(Optional)* In the **Settings** section, under **BASIC**, click **Chapters** and then review the structure of the results that will be created by the report. This structure cannot be modified.

8. At the bottom of the **Reports** page, click the **Save** button.

The new report appears in the list in the **My Reports** folder.
Edit an Existing Report (Classic Interface)

Required Tenable.io Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

Before You Begin

You can only modify a report if you are the owner, a user with an administrator account, or you have been given the Can configure permission for that report.

To modify an existing report:

1. In the top navigation bar, click Reports.

   The Reports page appears.

2. Do one of the following:

   - In the My Reports folder, click the row corresponding to the report that you want to configure.
   - In the All Reports folder, click the row corresponding to the report that you want to configure.

   The Report Results section appears, where Report Results is the name of the report you selected.
3. In the upper-right corner of the page, click the **Configure** button.

   The **Edit Report** section appears.

4. **Configure the settings for the report.**

5. At the bottom of the **Reports** page, click the **Save** button.

   The folder that contains the report appears, and the **Last Modified** date for the report is updated.
Run a Report (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

Before You Begin

Reports that are scheduled do not need to be run manually. However, if you want to run a scheduled report manually, the steps of this procedure are the same.

You can only run a report if you are the owner, a user with an administrator account, or you have been given the **Can control** or **Can configure** permission for that report.

To run a report:

1. In the top navigation bar, click **Reports**.
   
   The **Reports** page appears.

2. In the row corresponding to the report that you want to run, click the button.
   
   In that row, the image appears, indicating that the report is running.
View Report Results (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

**Before You Begin**

You can only view the results of a report if you are the owner, a user with an administrator account, or you have been given the **Can view**, **Can control**, or **Can configure** permission for that report.

**To view report results:**

1. In the top navigation bar, click **Reports**.
   
   The **Reports** page appears.

   ![Report Results](image1)

2. Do one of the following:
   
   - In the left pane, click **All Report Results**.
   
   The **All Report Results** section appears.

   ![Report Results](image2)
• Select the report that has results you want to view:

  a. In the left pane, click **My Reports** or **All Reports**.

  The folder appears.

  ![Image of My Reports folder]

  b. Click the row corresponding to the report that has results you want to view.

  The **Report Results** section appears, where Report Results is the name of the report you selected.

  ![Image of Report Results section]

3. In the row corresponding to the results that you want to view, click the **button.

The PDF that contains the results of the report is downloaded.

4. Open the PDF.

The results of the report appear.
CVE Analysis Report

January 25, 2017 at 7:28pm UTC
Delete a Report (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

Before a report is permanently deleted, it is moved to the Trash folder. While the report is in the Trash folder, it can no longer be run. However, you can still view the results of the report, or recover it. Once the report is permanently deleted, it cannot be recovered.

You can only delete a report if you are the owner or a user with an administrator account.

Deleted report results do not go to the Trash folder and can never be recovered.

**To delete a report:**

1. In the top navigation bar, click **Reports**.

   The Reports page appears.

2. In the row corresponding to the report that you want to delete, click the × button.

   The report is moved to the Trash folder. The report can still be recovered. If you want to permanently delete the report, continue with this procedure.

3. To permanently delete the report, on the left pane, click **Trash**.

   The Trash folder appears.
1. Do one of the following:

   - In the row corresponding to the report that you want to permanently delete, click the \( \times \) button.

   - If you want to permanently delete all reports that are in the **Trash** folder, in the upper-right corner, click the **Empty Trash** button.

The **Delete Reports** dialog box appears.

4. Click the **Delete** button.

   The report is permanently deleted and cannot be recovered.
Recover a Report (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

You can only recover a report if you are the owner or an administrator.

A permanently deleted report cannot be recovered.

To recover a report:

1. In the top navigation bar, click **Reports**.
   
   The Reports page appears.

2. In the left pane, click **Trash**.
   
   The Trash folder appears.

3. In the row corresponding to the report that you want to recover, click the check box.
   
   In the upper-right corner, the **More** drop-down box appears.
4. In the upper-right corner, click the **More** drop-down box, and point to **Move to**. Then, select the folder that you want the report to be moved to.

The report is recovered.
Delete Report Results (Classic Interface)

**Required Tenable.io Vulnerability Management User Role:** Standard, Scan Manager, or Administrator

You can only delete the results of a report if you are the owner, a user with an administrator account, or you have been given the Can control or Can configure permission for that report.

**Caution:** Report results are not sent to the Trash folder. When you delete the result of a report, it is permanently deleted and cannot be restored.

To delete report results:

1. In the top navigation bar, click Reports.

   The Reports page appears.

2. Do one of the following:
   - In the left pane, click All Report Results.

   The All Report Results section appears.
• Select the report that has results you want to view:

  a. In the left pane, click **My Reports** or **All Reports**.

     The folder appears.

     ![Image of My Reports folder]

     ![Image of CVE Analysis Report]

     b. Click the row corresponding to the report that has results you want to delete.

     The **Report Results** section appears, where Report Results is the name of the report you selected.

     ![Image of Report Results section]

3. In the row corresponding to the results that you want to delete, click the **×** button.

   The **Delete Report Result** dialog box appears.

   ![Image of Delete Report Result dialog box]

4. Click the **Delete** button.

   The report result is deleted.