**Table of Contents**

- **Welcome to Tenable.sc Director** ................................................................. 12
- Get Started With Tenable.sc Director .......................................................... 13
- Considerations for Air-Gapped Environments ........................................... 17
- Managing Tenable.sc Instances with Tenable.sc Director .......................... 19
- Connect a Managed Tenable.sc Instance ...................................................... 21
- Manage Your Tenable.sc Instances ............................................................. 23
- View Managed Tenable.sc Instances ........................................................... 24
- View Managed Tenable.sc Instance Details ............................................... 25
- Disconnect a Managed Tenable.sc Instance ............................................... 30
- Managed Tenable.sc Instance Settings ....................................................... 31
- Requirements ................................................................................................. 32
- Hardware Requirements ................................................................................ 33
- Cloud Requirements ..................................................................................... 36
- System Requirements ................................................................................... 39
- Customize SELinux Enforcing Mode Policies for Tenable.sc Director ........ 43
- Use /dev/random for Random Number Data Generation ........................... 44
- License Requirements .................................................................................. 45
- Apply a New License .................................................................................... 47
- Update an Existing License .......................................................................... 48
- Tenable.sc Director License Expiration ....................................................... 50
- Port Requirements ......................................................................................... 51
- Web Browser Requirements ......................................................................... 52
Tenable Integrated Product Compatibility .................................................. 53
Large Enterprise Deployments ................................................................. 54
Installation and Upgrade ............................................................................. 55
Before You Install ...................................................................................... 56
Install Tenable.sc Director .......................................................................... 58
  Quick Setup ............................................................................................ 60
Before You Upgrade ................................................................................... 63
Upgrade Tenable.sc Director ....................................................................... 65
Uninstall Tenable.sc Director ...................................................................... 68
User Access .................................................................................................. 69
Log In to the Web Interface ......................................................................... 70
  Log in to the Web Interface via SSL Client Certificate ............................... 72
User Roles ..................................................................................................... 75
  Create a User Role .................................................................................. 80
  Edit a User Role ..................................................................................... 81
  Delete a User Role .................................................................................. 83
Organizations and Groups .......................................................................... 84
Organizations ............................................................................................... 85
  Add an Organization ................................................................................ 89
  View Organization Details ...................................................................... 90
  Delete an Organization .......................................................................... 92
Groups .......................................................................................................... 93
  Add a Group ......................................................................................... 95
  Delete a Group ...................................................................................... 96
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Accounts</td>
<td>97</td>
</tr>
<tr>
<td>Add a TNS-Authenticated User</td>
<td>101</td>
</tr>
<tr>
<td>Add an LDAP-Authenticated User</td>
<td>103</td>
</tr>
<tr>
<td>Add a SAML-Authenticated User</td>
<td>106</td>
</tr>
<tr>
<td>Manage User Accounts</td>
<td>108</td>
</tr>
<tr>
<td>View User Details</td>
<td>109</td>
</tr>
<tr>
<td>Delete a User</td>
<td>111</td>
</tr>
<tr>
<td>Linked User Accounts</td>
<td>113</td>
</tr>
<tr>
<td>Add a Linked User</td>
<td>114</td>
</tr>
<tr>
<td>Switch to a Linked User Account</td>
<td>116</td>
</tr>
<tr>
<td>Delete a Linked User Account</td>
<td>117</td>
</tr>
<tr>
<td>Custom Group Permissions</td>
<td>119</td>
</tr>
<tr>
<td>Generate API Keys</td>
<td>121</td>
</tr>
<tr>
<td>Delete API Keys</td>
<td>123</td>
</tr>
<tr>
<td>LDAP Authentication</td>
<td>124</td>
</tr>
<tr>
<td>Add an LDAP Server</td>
<td>127</td>
</tr>
<tr>
<td>Delete an LDAP Server</td>
<td>128</td>
</tr>
<tr>
<td>LDAP Servers with Multiple OUs</td>
<td>129</td>
</tr>
<tr>
<td>SAML Authentication</td>
<td>133</td>
</tr>
<tr>
<td>Configure SAML Authentication Automatically via the User Interface</td>
<td>137</td>
</tr>
<tr>
<td>Configure SAML Authentication Manually via the User Interface</td>
<td>139</td>
</tr>
<tr>
<td>Configure SAML Authentication via the SimpleSAML Module</td>
<td>141</td>
</tr>
<tr>
<td>Configure SAML User Provisioning</td>
<td>145</td>
</tr>
<tr>
<td>SAML Authentication XML Configuration Examples</td>
<td>147</td>
</tr>
<tr>
<td>Chapter</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Certificate Authentication</td>
<td>151</td>
</tr>
<tr>
<td>Configure Tenable.sc Director to Allow SSL Client Certificate Authentication</td>
<td>152</td>
</tr>
<tr>
<td>Configure a CRL in Tenable.sc Director</td>
<td>154</td>
</tr>
<tr>
<td>Configure OCSP Validation in Tenable.sc Director</td>
<td>158</td>
</tr>
<tr>
<td>Certificates and Certificate Authorities in Tenable.sc Director</td>
<td>159</td>
</tr>
<tr>
<td>Tenable.sc Director Server Certificates</td>
<td>160</td>
</tr>
<tr>
<td>Upload a Server Certificate for Tenable.sc</td>
<td>161</td>
</tr>
<tr>
<td>Regenerate the Tenable.sc Director Server Certificate</td>
<td>164</td>
</tr>
<tr>
<td>Trust a Custom CA</td>
<td>165</td>
</tr>
<tr>
<td>System Settings</td>
<td>166</td>
</tr>
<tr>
<td>Configuration Settings</td>
<td>167</td>
</tr>
<tr>
<td>Edit Plugin and Feed Settings and Schedules</td>
<td>177</td>
</tr>
<tr>
<td>Configure Plugin Text Translation</td>
<td>179</td>
</tr>
<tr>
<td>API Key Authentication</td>
<td>180</td>
</tr>
<tr>
<td>Enable API Key Authentication</td>
<td>181</td>
</tr>
<tr>
<td>Disable API Key Authentication</td>
<td>182</td>
</tr>
<tr>
<td>Diagnostics Settings</td>
<td>183</td>
</tr>
<tr>
<td>Generate a Diagnostics File</td>
<td>184</td>
</tr>
<tr>
<td>Enable Touch Debugging</td>
<td>185</td>
</tr>
<tr>
<td>Disable Touch Debugging</td>
<td>186</td>
</tr>
<tr>
<td>Job Queue Events</td>
<td>187</td>
</tr>
<tr>
<td>System Logs</td>
<td>188</td>
</tr>
<tr>
<td>View System Logs</td>
<td>189</td>
</tr>
<tr>
<td>Publishing Sites Settings</td>
<td>190</td>
</tr>
</tbody>
</table>
External Repositories ................................................................. 227
Remote Repositories ................................................................. 228
Active Scan Objects ................................................................. 230
Assets ...................................................................................... 232
Add an Asset from a Template ................................................... 240
Add a Custom Asset ................................................................. 242
View Asset Details ................................................................. 243
Audit Files .................................................................................. 245
Add a Template-Based Audit File .............................................. 246
Add a Custom Audit File .......................................................... 247
Manage Audit Files ................................................................. 249
Scan Zones ................................................................................ 251
View Your Scan Zones ............................................................. 252
Tags ......................................................................................... 253
Add a Tag .................................................................................. 254
Remove or Delete a Tag ........................................................... 255

Analyze Data .............................................................................. 256
Dashboards ................................................................................ 257
View a Dashboard ..................................................................... 258
Insights Dashboard ................................................................... 260
Set a Dashboard as Your Default Dashboard ............................. 263
Share or Revoke Access to a Dashboard ..................................... 264
Delete a Dashboard ................................................................... 265
Add a Template-Based Dashboard ........................................... 266
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a Custom Dashboard</td>
<td>268</td>
</tr>
<tr>
<td>Import a Dashboard</td>
<td>269</td>
</tr>
<tr>
<td>Manage Dashboards</td>
<td>270</td>
</tr>
<tr>
<td>Manage Dashboard Components</td>
<td>272</td>
</tr>
<tr>
<td>Add a Template-Based Dashboard Component</td>
<td>274</td>
</tr>
<tr>
<td>Add a Custom Dashboard Component</td>
<td>276</td>
</tr>
<tr>
<td>Custom Dashboard Component Options</td>
<td>277</td>
</tr>
<tr>
<td>Configure a Simple Matrix Dashboard Component</td>
<td>285</td>
</tr>
<tr>
<td>Scan Results</td>
<td>289</td>
</tr>
<tr>
<td>Scan Result Statuses</td>
<td>290</td>
</tr>
<tr>
<td>Manage Scan Results</td>
<td>293</td>
</tr>
<tr>
<td>View Scan Results</td>
<td>296</td>
</tr>
<tr>
<td>View Scan Result Details</td>
<td>297</td>
</tr>
<tr>
<td>Solutions Analysis</td>
<td>299</td>
</tr>
<tr>
<td>View Solutions</td>
<td>300</td>
</tr>
<tr>
<td>View Solution Details</td>
<td>302</td>
</tr>
<tr>
<td>Vulnerability Analysis</td>
<td>304</td>
</tr>
<tr>
<td>Cumulative vs. Mitigated Vulnerabilities</td>
<td>305</td>
</tr>
<tr>
<td>View Cumulative or Mitigated Vulnerabilities</td>
<td>306</td>
</tr>
<tr>
<td>Severity vs. VPR</td>
<td>307</td>
</tr>
<tr>
<td>Vulnerability Analysis Tools</td>
<td>310</td>
</tr>
<tr>
<td>Vulnerability Analysis Filter Components</td>
<td>315</td>
</tr>
<tr>
<td>View Vulnerabilities by Host</td>
<td>326</td>
</tr>
<tr>
<td>View Vulnerabilities by Plugin</td>
<td>328</td>
</tr>
</tbody>
</table>
View Vulnerability Instance Details ............................................................. 331
View Host Details ....................................................................................... 333
View Plugin Details .................................................................................... 335
Export Vulnerability Data ........................................................................... 337
Reports ........................................................................................................ 338
Manage Reports .......................................................................................... 339
Create a Custom Report .............................................................................. 340
Create a Template Report ........................................................................... 342
Data Required for Template-Based Reports .............................................. 345
Edit a Report Definition ............................................................................ 346
Report Options .......................................................................................... 347
Edit a Report Outline ................................................................................. 355
Add a Custom Chapter to a Report ............................................................. 357
Add a Template Chapter to a Report ......................................................... 358
Add or Edit a Report Element .................................................................... 361
Configure a Grouping Element in a Report .............................................. 362
Configure a Text Element in a Report ....................................................... 366
Configure a Matrix Element in a Report ................................................... 369
Configure a Table Element in a Report ..................................................... 372
Configure a Charts Element in a Report .................................................. 375
Reorder Report Chapters and Elements .................................................. 379
Manage Filters for a Chapter Report .......................................................... 380
Manage Filter Components for a Single Element .................................... 381
Manage Filter Components for Multiple Elements .................................... 383
Manage Filter Components for a Non-Chapter Report ........................................... 385

View a Report Definition ....................................................................................... 387

Copy a Report Definition ....................................................................................... 388

Export a Report Definition ..................................................................................... 389

Import a Report Definition ..................................................................................... 390

Delete a Report Definition ..................................................................................... 391

Launch a Report on Demand ................................................................................... 392

Manage Report Results .......................................................................................... 393

Stop a Running Report ............................................................................................ 394

Download a Report Result ....................................................................................... 395

View a Report Result ............................................................................................... 396

Publish a Report Result .......................................................................................... 397

Email a Report Result ............................................................................................. 398

Copy a Report Result ............................................................................................. 399

View Errors for a Failed Report .............................................................................. 400

Delete a Report Result ............................................................................................ 401

CyberScope and DISA Report Attributes ............................................................... 402

Report Images ......................................................................................................... 405

Filters ...................................................................................................................... 407

Apply a Filter .......................................................................................................... 408

Queries ..................................................................................................................... 413

Add or Save a Query ............................................................................................... 417

Load a Query .......................................................................................................... 419

Workflow Actions ..................................................................................................... 420

Copyright © 2020 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.
Alerts .......................................................................................................................... 421
Tickets ....................................................................................................................... 426
Open a Ticket ............................................................................................................ 428

Additional Resources ............................................................................................... 430

Start, Stop, or Restart Tenable.sc Director ............................................................... 431
License Declarations ................................................................................................. 432
Encryption Strength .................................................................................................. 433
  Configure SSL/TLS Strong Encryption .................................................................. 435
Perform an Offline Tenable.sc Director Plugin/Feed Updates ............................... 436
  Perform an Offline Nessus Plugin Update ............................................................... 437
  Perform an Offline NNM Plugin Update ................................................................. 439
  Perform an Offline Tenable.sc Feed Update ............................................................ 441
Troubleshooting ........................................................................................................ 443
  General Tenable.sc Director Troubleshooting ....................................................... 444
Welcome to Tenable.sc Director

This user guide describes how to install, configure, and manage Tenable.sc Director™ 5.17.x.

Tenable.sc Director is an add-on to Tenable.sc that provides centralized management and scanning capabilities to reduce complexity and give multiple-console customers complete visibility across their entire network.

To get started, see Get Started With Tenable.sc Director.
Get Started With Tenable.sc Director

Use the following getting started sequence to configure and mature your Tenable.sc Director deployment. A fully configured Tenable.sc Director deployment includes one Tenable.sc Director and one or more managed Tenable.sc instances. For more information, see Managing Tenable.sc Instances with Tenable.sc Director.

1. Prepare
2. Configure Managed Tenable.sc Instances
3. Install
4. Monitor Scans
5. Refine
6. Expand

Prepare

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

- Design a deployment plan by identifying your organization's objectives and analyzing your network topology. Consider Tenable-recommended best practices for your environment.

  Note: Tenable.sc Director cannot perform scans. Plan your deployment to ensure adequate you have adequate scan coverage on the Tenable.sc instances you plan to connect to and monitor from Tenable.sc Director.

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

For more information about planning a large enterprise deployment of Tenable.sc, see the Tenable.sc Large Enterprise Deployment Guide.

Configure Managed Tenable.sc Instances

Configure the Tenable.sc instances you want to manage with Tenable.sc Director.
1. Install and fully configure Tenable.sc on your managed Tenable.sc instances, as described in Get Started With Tenable.sc in the Tenable.sc User Guide.

2. Apply the required license upgrade to each managed Tenable.sc instance, as described in Update an Existing License.

3. Generate API keys for an administrator on each managed Tenable.sc instance, as described in Generate API Keys.

**Install**

Install Tenable.sc Director and perform initial configuration.

*Note:* You cannot upgrade Tenable.sc to Tenable.sc Director. If you want to install Tenable.sc Director on a host where Tenable.sc is already installed, you must uninstall Tenable.sc and perform a clean installation of Tenable.sc Director on that host.

1. Prepare for the installation, as described in Before You Install.

2. Install Tenable.sc Director, as described in Install Tenable.sc Director.

3. Perform quick setup, as described in Quick Setup. You can:
   - Apply activation codes for Nessus, NNM, and LCE
   - Connect Tenable.sc instances you want to manage with Tenable.sc Director
   - Create one organization
   - Create one administrator user account and one security manager account
   - Configure usage statistic collection

   Tenable recommends following the quick setup wizard, but you can configure these features later. For example, do not configure LDAP until you have easy access to all necessary LDAP parameters.

4. Configure SMTP settings, as described in Mail Settings.

5. Configure remote repositories, if necessary, as described in Repositories.

6. Configure security settings (e.g., password complexity requirements and custom banners), as described in Security Settings.
7. Configure and connect additional managed Tenable.sc instances, if necessary, as described in Connect a Managed Tenable.sc Instance.

Monitor Scans

On your managed Tenable.sc instances, configure and run basic scans to begin evaluating the effectiveness of your deployment plan and analysis workflow, as described in Getting Started with Tenable.sc in the Tenable.sc User Guide.

- Monitor running scans and scanner availability using the Insights Dashboard.
- When the scans complete, create template-based dashboards and reports, as described in Dashboards and Reports.

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.

- Configure audit files, as described in Audit Files.
- Configure groups, as described in Add a Group.
- Create a custom user role, as described in Create a User Role.
- Create additional user accounts and share objects with users, as described in User Accounts.
- Create dynamic assets and combination assets, as described in Add a Custom Asset. For more information about asset types, see Assets.
- Review the plugin update schedule, as described in Edit Plugin and Feed Settings and Schedules. Consider editing the schedules to suit your needs. For example, you may want to schedule plugin and feed updates to run a few hours before your scheduled scans.
- Add queries and use filters, as described in Add or Save a Query and Apply a Filter.
- Create custom dashboards and reports, as described in Dashboards and Reports.
- Configure alerts and ticketing, as described in Workflow Actions.
• View vulnerability data and use the built-in analysis tools, as described in *Vulnerability Analysis*.

**Expand**

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 scan automation settings on your managed Tenable.sc instances and consider revising.

• Review your scan results and scan coverage. You may need to modify your scan configurations on your managed Tenable.sc instances 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.

• Optimize and operationalize your custom reports to prepare them for distribution.

• Consider configuring API integrations, as described in the *Tenable.sc API Guide* and the *Tenable.sc API Best Practices Guide*. 
Considerations for Air-Gapped Environments

Consider the following when deploying Tenable.sc in an air-gapped (offline) environment.

Architecture

You must deploy a Tenable.sc and a set of scanners within each air-gapped network.

If you want to consolidate data from other networks with the data generated in your air-gapped network, you can use offline repositories to export data from your air-gapped Tenable.sc to your other instance of Tenable.sc. This supports both consolidated and federated reporting structures.

Upgrades and Updates

Tenable recommends performing Tenable.sc upgrades at least once a year (quarterly preferred) and plugin/feed updates at least once a month. After you perform a plugin update, run comprehensive scans to take advantage of the new vulnerability data and generate current scan results.

Note: A few plugins require internet access and cannot run in an air-gapped environment. For example, Nessus plugin 52669 checks to see if a host is part of a botnet.

After you perform a plugin update or feed update, verify the files as described in the knowledge base article.

To perform a Tenable.sc upgrade or a plugin/feed update offline:

Tip: You can use the API to automate some Tenable.sc upgrade and plugin update process.

1. Download the files in a browser or via the API.
2. Verify the integrity of the files.
   - Tenable.sc upgrade: Compare the download checksum with the checksum on the Tenable downloads page
   - Plugin/feed update: Download and compare the checksums.
3. Move the files to your Tenable.sc instance.
4. Upload the files to Tenable.sc.
   - Tenable.sc upgrade: [via the CLI](#).
   - Plugin/feed update: [in a browser](#) or [via the API](#).

### Nessus Agents

If you deployed Nessus Manager to manage Nessus Agents in an air-gapped environment, perform an offline software update (nessus-agent-updates-X.X.X.tar.gz on the [Tenable Downloads](#) site) on your Nessus Manager. Nessus Manager pushes the update to the managed Nessus Agents.

For more information, see the [knowledge base](#) article.
Managing Tenable.sc Instances with Tenable.sc Director

You can connect managed Tenable.sc instances to Tenable.sc Director to monitor Nessus scanners, scan zones, and scan results on multiple Tenable.sc instances from Tenable.sc Director. If your deployment includes several instances of Tenable.sc, Tenable recommends using Tenable.sc Director to remotely monitor your Tenable.sc instances.

A tiered Tenable.sc instances configuration includes:

- One **Tenable.sc Director instance** where you connect managed Tenable.sc instances. You use this instance to centralize and monitor data collected by your managed Tenable.sc instances.

  **Note:** Tenable.sc Director cannot perform scans. Plan your deployment to ensure adequate you have adequate scan coverage on the Tenable.sc instances you plan to connect to and monitor from Tenable.sc Director.

- One or more **managed Tenable.sc instances**. You connect managed Tenable.sc instances to collect vulnerability data that can be viewed in Tenable.sc Director.

  **Note:** You cannot edit configurations on managed Tenable.sc instances from Tenable.sc Director. To manage Nessus scanners, scan zones, scan results, and other configurations on a managed Tenable.sc instance, log in to that instance.

  **Note:** You cannot download Nessus scanner logs on managed Tenable.sc instances from Tenable.sc Director. To download Nessus scanner logs on a managed Tenable.sc instance, log in to that instance.

When you configure Tenable.sc Director and connect one or more managed Tenable.sc instances, you can monitor the following details from Tenable.sc Director:

- The status and version of Nessus running on the scanners on each managed Tenable.sc instance
- The total number of [Nessus Scanners](#) on each managed Tenable.sc instance
- The [Scan Zones](#) configured on each managed Tenable.sc instance
- The [scan results](#) of scans run on each managed Tenable.sc instance
• A summary of plugin sets used on each managed Tenable.sc instance
• A summary of plugin sets used by Nessus scanners on each managed Tenable.sc instance
• The version of Tenable.sc running on each managed Tenable.sc instance

From Tenable.sc Director, you can pause, resume, and stop scans that are running on managed Tenable.sc instances. For more information, see Start, Pause, or Stop Scans on a Managed Tenable.sc Instance.

For more information, see:

• Get Started With Tenable.sc Director
• Manage Your Tenable.sc Instances

Tip: Managed Tenable.sc instances cannot share repository data. For more information about sharing repository data between Tenable.sc instances, see Tiered Remote Repositories.
Connect a Managed Tenable.sc Instance

**Required User Role:** Tenable.sc Director Administrator

For more information about connecting Tenable.sc instances to Tenable.sc Director, see [Managing Tenable.sc Instances with Tenable.sc Director](#).

Before you begin:

- Generate API keys for an administrator on the Tenable.sc instance you want to manage with Tenable.sc Director, as described in [Generate API Keys](#).

To connect a Tenable.sc instance to Tenable.sc Director:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Managed Instances**.
   
   The **Tenable.sc Instances** page appears.
3. Click the **Add** button.
   
   The **Add Tenable.sc Instance** page appears.
4. Configure the options for the managed Tenable.sc instance. For more information, see [Managed Tenable.sc Instance Settings](#).
   
   a. In the **Name** box, type a name.
   b. In the **Port** box, type the HTTPS port (typically, 443).
   c. In the **IP Address** box, type the IP address.
   d. (Optional) In the **Description** box, type a description.
   e. In the **Access Key** box, type the API access key for an administrator.
   f. In the **Secret Key** box, type the API secret key for an administrator.
   g. (Optional) To verify that the IP address entered in the **IP Address** option matches the CommonName (CN) presented in the SSL certificate from the Tenable.sc instance, click **Verify Hostname** to enable the toggle.
h. (Optional) To use the proxy configured in Tenable.sc Director for communication with the Tenable.sc instance, click **Use Proxy** to enable the toggle.

5. Click **Submit**.

Tenable.sc Director saves your configuration.

What to do next:

- Begin monitoring data on your managed Tenable.sc instances.
  - To view the Nessus scanners, scan zones, and scan results on a managed Tenable.sc instance, see [View Managed Tenable.sc Instance Details](#).
  - To view the Nessus scanners on your managed Tenable.sc instances, see [View Your Nessus Scanners](#).
  - To view the scan zones on your managed Tenable.sc instances, see [View Your Scan Zones](#).
  - To view the scan results on your managed Tenable.sc instances, see [View Scan Results](#).
Manage Your Tenable.sc Instances

Required User Role: Tenable.sc Director Administrator

For more information, see Managing Tenable.sc Instances with Tenable.sc Director.

To manage your linked Tenable.sc instances:

1. Log in to Tenable.sc Director via the user interface.
2. Click Managed Instances.
   The Tenable.sc Instances page appears.
3. To view the list and status of your managed Tenable.sc instances, see View Managed Tenable.sc Instances.
4. To view details for a managed Tenable.sc instance, see View Managed Tenable.sc Instance Details.
5. To edit the name or description of a managed Tenable.sc instance:
   a. In the row for the managed Tenable.sc instance you want to edit, click the menu.
      The actions menu appears.
   b. Click Edit.
      The Edit Tenable.sc Instance page appears.
   c. Modify the managed Tenable.sc instance options. For more information, see Managed Tenable.sc Instance Settings.
   d. Click Submit.
      Tenable.sc Director saves your configuration.
6. To disconnect a managed Tenable.sc instance, see Disconnect a Managed Tenable.sc Instance.
View Managed Tenable.sc Instances

**Required User Role:** Tenable.sc Director Administrator

To view details for a managed Tenable.sc instance, see View Managed Tenable.sc Instance Details.

For more information, see Managing Tenable.sc Instances with Tenable.sc Director.

To view a list of your managed Tenable.sc instances:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Managed Instances**.
   
   The **Tenable.sc Instances** page appears.
3. View the following information about each managed Tenable.sc instance:

   - **Name** — The name of the instance.
   - **IP/FQDN** — The IP address of the instance.
   - **Version** — The version of Tenable.sc running on the instance.
   - **Status** — The status of the scanners on the instance.
   - **Scanners** — The number of available scanners compared to the total number of scanners on the managed Tenable.sc instance.
   - **Last Sync** — The length of time since the last successful synchronization of the managed Tenable.sc instance.

   *Note: Your primary Tenable.sc instance is named Local in this list.*
View Managed Tenable.sc Instance Details

**Required User Role:** Tenable.sc Director Administrator

From Tenable.sc Director, you can view details about each managed Tenable.sc instance, including all Nessus scanners, scan zones, and scan results.

For more information about managing Tenable.sc instances with Tenable.sc Director, see [Managing Tenable.sc Instances with Tenable.sc Director](#).

To view details for a managed Tenable.sc instance:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Managed Instances**.
   
   The **Tenable.sc Instances** page appears.
3. In the row for the managed Tenable.sc instance, click the **menu**.
   
   The actions menu appears.
4. Click **View**.
   
   The managed Tenable.sc instance page appears.
5. To view configuration details for the managed Tenable.sc instance:
   
   a. Click the **Information** tab.
      
      The **Information** tab loads.
   
   b. View the following information for the managed Tenable.sc instance:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>View general information about the managed Tenable.sc instance.</td>
</tr>
<tr>
<td>Options</td>
<td>View optional settings configured for the managed Tenable.sc instance.</td>
</tr>
<tr>
<td>Scanner Summary</td>
<td>View a summary of the scanners configured on the managed Tenable.sc instance.</td>
</tr>
</tbody>
</table>

---

Copyright © 2020 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.
- **Scanner Version** — The total number of Nessus scanners on the instance, organized by Nessus scanner version.

- **Scanner Status** — The total number of Nessus scanners on the instance, organized by status.

- **Scanner PluginSet** — The total number of Nessus scanners on the instance, organized by scanner pluginset.

6. To view the Nessus scanners configured on the managed Tenable.sc instance:

   a. Click the **Scanners** tab.

   The **Scanners** tab loads.

   b. View the following information about the Nessus scanners configured on the instance:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanners table</td>
<td>- View the number of operational Nessus scanners compared to the total number of scanners on the managed Tenable.sc instance.</td>
</tr>
<tr>
<td></td>
<td>- View the Nessus scanners on the managed Tenable.sc instance.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Name</strong> — The name for the scanner.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Tenable.sc Instance</strong> — The name of the Tenable.sc instance where the scanner is configured. For more information, see <a href="#">Managing Tenable.sc Instances with Tenable.sc Director</a>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Features</strong> — Specifies whether the scanner is a <strong>Standard</strong> scanner or an <strong>Agent Capable</strong> scanner. Agent capable scanners provide Nessus Agent scan results to Tenable.sc.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Status</strong> — The status of the scanner.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Host</strong> — The IP address or hostname of the scanner.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Version</strong> — The scanner’s Nessus version.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type</strong> — The type of scanner connection: <strong>Nessus (Unman-</strong></td>
</tr>
</tbody>
</table>
7. To view the scan zones configured on the managed Tenable.sc instance:
   a. Click the **Scan Zones** tab.
      
The **Scan Zones** tab loads.
   b. View the following information about the scan zones configured on the instance:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Zones table</td>
<td>• View the number of operational scan zones on the managed Tenable.sc instance.</td>
</tr>
<tr>
<td></td>
<td>• View the scan zones on the managed Tenable.sc instance.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong> — The name for the scan zone.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Tenable.sc Instance</strong> — The name of the Tenable.sc instance where your scan zone is configured. For more information, see <strong>Managing Tenable.sc Instances with Tenable.sc Director</strong>.</td>
</tr>
</tbody>
</table>
- Status — The status of the scan zone. For more information, see View Your Scan Zones.

- Scanners — The number of Nessus scanners in the scan zone.

- Last Modified — The date and time the scan zone was last modified.

  View details for a scan zone configured on the managed Tenable.sc instance.

  1. Click the menu in the row for the scan zone you want to view.

     The actions menu appears.

  2. Click View.

     The View Scan Zone page appears. For more information, see View Your Scan Zones.

8. To view the results of scans run on the managed Tenable.sc instance:

   a. Click the Scan Results tab.

      The Scan Results tab loads.

   b. View the following information about the results of scans run on the instance:

      | Section          | Action                                                                 |
      |------------------|------------------------------------------------------------------------|
      | Scan Results table | View the scan results on the managed Tenable.sc instance.                |
      |                  | • Name — The name for the scan associated with the result.             |
      |                  | • Tenable.sc Instance — The name of the Tenable.sc instance where the scan was run. |
      |                  | • Type — The type of scan that generated the scan result.              |
      |                  | • Scan Policy Plugins — The name of the scan policy that generated the scan result. |
      |                  | • Scanned IPs — The number of IP addresses scanned.                    |
- Group — The group associated with the scan.
- Owner — The username for the user who added the scan.
- Duration — The total time elapsed while running the scan.
- Import Time — The date and time Tenable.sc completed the scan result import.
- Status — The status of the scan that generated the scan result.

For more information, see Scan Status.

**Note:** You can view scan results from managed Tenable.sc instances from the past 7 days. To view older scan results, log in to the managed Tenable.sc instance where the scan took place.

- **View details for a scan result on the managed Tenable.sc instance.**
  1. Click the row for the scan result you want to view.
     
     The View Scan Zone page appears. For more information, see View Scan Result Details.

9. **To view details for a different managed Tenable.sc instance:**
   
   a. Click the Jump to... menu.
      
      The list of managed Tenable.sc instances appears.
   
   b. Click the name of the managed Tenable.sc instance you want to view.
      
      The View Tenable.sc Instance page appears.
Disconnect a Managed Tenable.sc Instance

**Required User Role:** Tenable.sc Director Administrator

Disconnect a managed Tenable.sc instance from Tenable.sc Director to stop monitoring the instance from Tenable.sc Director. You can continue using individual Tenable.sc instances separately from Tenable.sc Director. For more information, see Managing Tenable.sc Instances with Tenable.sc Director.

To disconnect a managed Tenable.sc instance:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Managed Instances**.
   - The **Tenable.sc Instances** page appears.
3. In the row for the managed Tenable.sc instance you want to disconnect, click the menu.
   - The actions menu appears.
4. Click **Delete**.
   - A confirmation window appears.
5. Click **Delete**.
   - Tenable.sc Director disconnects the managed Tenable.sc instance.
# Managed Tenable.sc Instance Settings

For more information, see [Managing Tenable.sc Instances with Tenable.sc Director](#) and [Configure Tier Management of Tenable.sc Instances](#).

The following table describes the options to configure when connecting managed Tenable.sc instances.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A descriptive name for the Tenable.sc instance.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the Tenable.sc instance.</td>
</tr>
<tr>
<td>Port</td>
<td>The TCP port that the Tenable.sc instance listens on for communications from Tenable.sc (443).</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) A description for the Tenable.sc instance.</td>
</tr>
<tr>
<td><strong>API Keys</strong></td>
<td></td>
</tr>
<tr>
<td>Access Key</td>
<td>The API access key for an administrator user on the managed Tenable.sc instance. For more information, see <a href="#">Generate API Keys</a>.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>The API secret key for an administrator user on the managed Tenable.sc instance. For more information, see <a href="#">Generate API Keys</a>.</td>
</tr>
<tr>
<td><strong>Options</strong></td>
<td></td>
</tr>
<tr>
<td>Verify Hostname</td>
<td>(Optional) When enabled, adds a check to verify that the IP address entered in the IP Address option matches the CommonName (CN) presented in the SSL certificate from the managed Tenable.sc instance.</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>(Optional) When enabled, instructs Tenable.sc Director to use its configured proxy for communication with the managed Tenable.sc instance.</td>
</tr>
</tbody>
</table>
Requirements

Tenable.sc Director is supported in physical hardware and cloud environments.

For more information, see:

- Hardware Requirements
- Cloud Requirements
- System Requirements
- License Requirements
- Port Requirements
- Web Browser Requirements
- Tenable Integrated Product Compatibility
- Large Enterprise Deployments
Hardware Requirements

Use the following hardware recommendations for Tenable.sc as a guide when preparing your physical or Tenable Core environment.

**Note:** Tenable strongly discourages deploying Tenable.sc or Tenable Core + Tenable.sc in an environment shared with other Tenable applications.

Storage Requirements

Tenable recommends installing Tenable.sc on direct-attached storage (DAS) devices (or storage area networks [SANs], if necessary) with a storage latency of 10 milliseconds or less.

Tenable does not support installing Tenable.sc on network-attached storage (NAS).

Disk Space Requirements

Enterprise networks can vary in performance, capacity, protocols, and overall activity. Resource requirements to consider for deployments include raw network speed, the size of the network being monitored, and the configuration of the application. Processors, memory, and network cards will be heavily based on the former. Disk space requirements will vary depending on usage based on the amount and length of time data is stored on the system.

An important consideration is that Tenable.sc can be configured to save a snapshot of vulnerability archives each day. In addition, the size of the vulnerability data stored by Tenable.sc depends on the number and types of vulnerabilities, not just the number of hosts. For example, 100 hosts with 100 vulnerabilities each could consume as much data as 1,000 hosts with 10 vulnerabilities each. In addition, the output for vulnerability check plugins that do directory listings, etc. is much larger than Open Port plugins from discovery scans.

For networks of 35,000 to 50,000 hosts, Tenable has encountered data sizes of up to 25 GB. That number is based on storage of 50,000 hosts and approximately 500 KB per host.

Additionally, during active scanning sessions, large scans and multiple smaller scans have been reported to consume as much as 150 GB of disk space as results are acquired. Once a scan has completed and its results are imported, that disk space is freed up.

Requirements When Running Basic Network Scans + Local Checks
<table>
<thead>
<tr>
<th>Version</th>
<th># of Hosts Managed by Tenable.sc</th>
<th>CPU Cores</th>
<th>Memory</th>
<th>Disk Space used for Vulnerability Trending</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2,500 active IPs</td>
<td>4 2GHz cores</td>
<td>8 GB RAM</td>
<td>90 days: 125 GB 180 days: 250 GB</td>
</tr>
<tr>
<td>5.x</td>
<td>10,000 active IPs</td>
<td>8 3GHz cores</td>
<td>16 GB RAM</td>
<td>90 days: 450 GB 180 days: 900 GB</td>
</tr>
<tr>
<td></td>
<td>25,000 active IPs</td>
<td>16 3GHz cores</td>
<td>32 GB RAM</td>
<td>90 days: 1.2 TB 180 days: 2.4 TB</td>
</tr>
<tr>
<td></td>
<td>100,000 active IPs</td>
<td>32 3GHz cores</td>
<td>64 GB RAM</td>
<td>90 days: 4.5 TB 180 days: 9 TB</td>
</tr>
</tbody>
</table>

Requirements When Running Basic Network Scans + Local Checks + 1 Configuration Audit

<table>
<thead>
<tr>
<th>Version</th>
<th># of Hosts Managed by Tenable.sc</th>
<th>CPU Cores</th>
<th>Memory</th>
<th>Disk Space used for Vulnerability Trending</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.x</td>
<td>2,500 active IPs</td>
<td>4 2GHz cores</td>
<td>8 GB RAM</td>
<td>90 days: 225 GB 180 days: 450 GB</td>
</tr>
<tr>
<td></td>
<td>10,000 active IPs</td>
<td>8 3GHz cores</td>
<td>16 GB RAM</td>
<td>90 days: 900 GB 180 days: 1.8 TB</td>
</tr>
<tr>
<td></td>
<td>25,000 active IPs</td>
<td>16 3GHz cores</td>
<td>32 GB RAM</td>
<td>90 days: 2.25 TB</td>
</tr>
<tr>
<td>Version</td>
<td># of Hosts Managed by Tenable.sc</td>
<td>CPU Cores</td>
<td>Memory</td>
<td>Disk Space used for Vulnerability Trending</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------</td>
<td>-----------</td>
<td>--------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cores</td>
<td></td>
<td>180 days: 4.5 TB</td>
</tr>
<tr>
<td></td>
<td>100,000 active IPs</td>
<td>32 3GHz</td>
<td>128 GB RAM</td>
<td>90 days: 9 TB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cores</td>
<td></td>
<td>180 days: 18 TB</td>
</tr>
</tbody>
</table>

**Disk Partition Requirements**

Tenable.sc installs into `/opt/sc`. Tenable highly recommends that you create the `/opt` directory on a separate disk partition. If you want to increase performance, consider using two disks: one for the operating system and one for the system deployed to `/opt`.

Tenable strongly recommends using high performance disks. Tenable.sc is a disk-intensive application and using disks with high read/write speeds, such as SSDs, results in the best performance.

If required disk space exists outside of the `/opt` file system, mount the desired target directory using the command `mount --bind <olddir> <newdir>`. Make sure that the file system is automatically mounted on reboot by editing the `/etc/fstab` file appropriately.

**Note:** Tenable.sc does not support using symbolic links for `/opt/sc/`. You can use symbolic links within `/opt/sc/` subdirectories if instructed by Tenable.sc documentation or Tenable Support.

Deploying Tenable.sc on a server configured with RAID disks can also dramatically boost performance.

**Tip:** Tenable does not require RAID disks for even our largest customers. However, in one instance, response times for queries with a faster RAID disk for a customer with more than 1 million managed vulnerabilities moved from a few seconds to less than a second.

**Network Interface Requirements**

You can install Tenable.sc in externally connected or air-gapped environments. For more information about special considerations for air-gapped environments, see [Considerations for Air-Gapped Environments](#).

Gigabit or faster network cards are recommended for use on the Tenable.sc server. This is to increase the overall performance of web sessions, emails, LCE queries, and other network activities.
Cloud Requirements

You can install Tenable.sc in cloud-based environments using the same hardware recommendations for an on-premise installation of Tenable.sc.

You must install Tenable.sc in a vendor-supported version of your cloud environment that meets the operating system requirements to run Tenable.sc.

The following guidelines can help you install Tenable.sc in an Amazon Elastic Compute Cloud (Amazon EC2) cloud-based environment, but they do not cover all deployment scenarios or cloud environments. For assistance with a different cloud environment, contact Tenable Professional Services.

- **Supported Amazon EC2 Instance Types**
- **Supported Amazon Machine Images (AMIs)**

**Supported Amazon EC2 Instance Types**

You can install Tenable.sc in an Amazon Elastic Compute Cloud (Amazon EC2) cloud-based environment that meets all of the following requirements.

Tenable.sc uses a balance of networking and compute resources and requires persistent storage for proper operation. To meet these requirements, Tenable supports installing Tenable.sc on M5 instances with General Purpose SSD (gp2) EBS storage.

Tenable recommends the following Amazon EC2 instance types based on your Tenable.sc deployment size.

**Requirements When Running Basic Network Scans + Local Checks**

<table>
<thead>
<tr>
<th># of Hosts Managed by Tenable.sc</th>
<th>EC2 Instance Type</th>
<th>Disk Space Used for Vulnerability Trending</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 2,500</td>
<td>m5.2xlarge</td>
<td>90 days: 125 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>180 days: 250 GB</td>
</tr>
<tr>
<td>2,501 to 10,000</td>
<td>m5.4xlarge</td>
<td>90 days: 450 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>180 days: 900 GB</td>
</tr>
<tr>
<td>10,001 to 25,000</td>
<td>m5.8xlarge</td>
<td>90 days: 1.2 TB</td>
</tr>
</tbody>
</table>
### Requirements When Running Basic Network Scans + Local Checks + 1 Configuration Audit

<table>
<thead>
<tr>
<th># of Hosts Managed by Tenable.sc</th>
<th>EC2 Instance Type</th>
<th>Disk Space Used for Vulnerability Trending</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 2,500</td>
<td>m5.4xlarge</td>
<td>90 days: 225 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>180 days: 450 GB</td>
</tr>
<tr>
<td>2,501 to 10,000</td>
<td>m5.8xlarge</td>
<td>90 days: 900 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>180 days: 1.8 TB</td>
</tr>
<tr>
<td>10,001 to 25,000</td>
<td>m5.8xlarge</td>
<td>90 days: 2.25 TB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>180 days: 4.5 TB</td>
</tr>
<tr>
<td>25,001 to 50,000</td>
<td>m5.12xlarge</td>
<td>90 days: 9 TB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>180 days: 18 TB</td>
</tr>
<tr>
<td>50,001 or more</td>
<td></td>
<td>For assistance with large enterprise deployments greater than 50,000 active IP addresses, contact your Tenable representative.</td>
</tr>
</tbody>
</table>

### Supported Amazon Machine Images (AMIs)

Tenable does not provide an AMI customized for Tenable.sc. Tenable supports using the following Amazon Marketplace AMI for Tenable.sc:

**AMI** | **Required Configuration Changes**
--- | ---
CentOS 7 (x86_64) - with | * This AMI does not include Java, but Tenable.sc requires OpenJDK or the Oracle Java JRE to export PDF reports.
<table>
<thead>
<tr>
<th>Updates HVM</th>
<th>You must install OpenJDK or the Oracle Java JRE onto your AMI before hosting Tenable.sc. For more information, see Dependencies.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• This AMI configures an SELinux enforcing mode policy, which requires customization to be compatible with Tenable.sc.</td>
</tr>
<tr>
<td></td>
<td>You must use the SELinux <code>sealert</code> tool to identify errors and solutions. For more information, see Customize SELinux Enforcing Mode Policies for Tenable.sc.</td>
</tr>
<tr>
<td></td>
<td>• You must confirm this AMI meets all other standard requirements for operating systems. For more information, see Operating System Requirements.</td>
</tr>
</tbody>
</table>
System Requirements

- Operating System Requirements
- SELinux Requirements
- Secure Environment Requirements
- Dependencies
- Tenable.sc Communications and Directories

Operating System Requirements

This version of Tenable.sc is available for:

- Red Hat Enterprise Linux 7 (RHEL 7), 64-bit
- Red Hat Enterprise Linux 8 (RHEL 8), 64-bit
- CentOS 7, 64-bit
- CentOS 8, 64-bit

SELinux Requirements

Tenable.sc supports disabled, permissive, and enforcing mode Security-Enhanced Linux (SELinux) policy configurations.

- Disabled and permissive mode policies typically do not require customization to interact with Tenable.sc.

- Enforcing mode policies require customization to interact with Tenable.sc. For more information, see Customize SELinux Enforcing Mode Policies for Tenable.sc Director.

Note: Tenable recommends testing your SELinux configurations before deploying on a live network.

Secure Environment Requirements

Tenable recommends adhering to security best practices, including:
Configure the operating system to ensure that security controls cannot be bypassed.

Configure the network to ensure that the Tenable.sc system resides in a secure network segment that is not accessible from the Internet.

Configure network time synchronization to ensure that accurate time stamps are recorded in reports and log files.

Note: The time zone is set automatically during the installation process with no user interaction. The time zone configured in php.ini must be synchronized with the system time zone in /etc/sysconfig/clock.

Configure access control to ensure that only authorized users have access to the operating system platform.

Monitor system resources to ensure that adequate disk space and memory are available, as described in Hardware Requirements. If system resources are exhausted, Tenable.sc may not log audit data during system administrator troubleshooting or other activities. For more information about troubleshooting resource exhaustion, see General Tenable.sc Director Troubleshooting.

For information about secure administration of a Red Hat installation, see the Red Hat Enterprise Linux Security Guide for your version.

Note: Even though the security concepts from this guide are written for RHEL 6, most of the concepts and methodologies apply to earlier versions of RHEL that are supported with Tenable.sc.

Note: As with any application, the security and reliability of the installation is dependent on the environment that supports it. It is strongly recommended that organizations deploying Tenable.sc have an established and applied IT management policy that covers system administration integrity, resource monitoring, physical security, and disaster recovery.

Dependencies

Note: Either OpenJDK or the Oracle Java JRE along with their accompanying dependencies must be installed on the system along with any additional Java installations removed for reporting to function properly.

Note: Tenable does not recommend forcing the installation without all required dependencies. If your version of Red Hat or CentOS is missing certain dependencies, it will cause problems that are not read-
It is apparent with a wide variety of functions. Tenable Support has observed different types of failure modes for Tenable.sc when dependencies are missing.

All dependencies must be installed on the system prior to installing the Tenable.sc package. While they are not all required by the installation RPM file, some functionality of Tenable.sc may not work properly if the packages are not installed.

**Note:** Using the latest stable production version of each package is recommended.

For a list of required packages, run the following command against the Tenable.sc RPM file:

```
# rpm -qp SecurityCenter-x.x.x-el6.x86_64.rpm --requires
```

- or -

```
# rpm -qp SecurityCenter-x.x.x-el7.x86_64.rpm --requires
```

To determine which version of a dependency is installed on your system, run the following command for each of the packages (replace “libtool” with the appropriate package):

```
# rpm -qa | grep libtool
```

If one of the prerequisite packages is missing, it can be installed using the “yum” or “rpm” package managers. For example, install Java 1.7.0 with “yum” using the command below:

```
# yum -y install java-1.7.0-openjdk.x86_64
```

### Tenable.sc Communications and Directories

The following table summarizes the components’ primary directories and communication methods.

**Note:** Tenable.sc does not support using symbolic links for `/opt/sc/`. You can use symbolic links within `/opt/sc/` subdirectories if instructed by Tenable.sc documentation or Tenable Support.

<table>
<thead>
<tr>
<th>Tenable.sc Directories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Directory</td>
</tr>
<tr>
<td><code>/opt/sc</code></td>
</tr>
</tbody>
</table>
# Tenable.sc Directories

<table>
<thead>
<tr>
<th>Directory</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Data</td>
<td>/opt/sc/orgs/&lt;Organization Serial Number&gt;</td>
</tr>
<tr>
<td>Repositories</td>
<td>/opt/sc/repositories/&lt;Repository Number&gt;</td>
</tr>
<tr>
<td>Admin Logs</td>
<td>/opt/sc/admin/logs/</td>
</tr>
<tr>
<td>Organization Logs</td>
<td>/opt/sc/orgs/&lt;Organization Number&gt;/logs/</td>
</tr>
</tbody>
</table>

**Communication Interfaces**

- User Access — HTTPS
- Feed Updates — Acquired over SSL from Tenable servers directly to Tenable.sc or for offline installation. Plugin packages are secured via 4096-bit RSA digital signatures.

For more information, see [Port Requirements](#).

For information about data encryption in Tenable.sc, see [Encryption Strength](#).
Customize SELinux Enforcing Mode Policies for Tenable.sc Director

Security-Enhanced Linux (SELinux) enforcing mode policies require customization to interact with Tenable.sc Director.

Tenable Support does not assist with customizing SELinux policies, but Tenable recommends monitoring your SELinux logs to identify errors and solutions for your policy configuration.

Before you begin:

- Install the SELinux `sealert` tool in a test environment that resembles your production environment.

To monitor your SELinux logs to identify errors and solutions:

1. Run the `sealert` tool, where `/var/log/audit/audit.log` is the location of your SELinux audit log:

   ```bash
   sealert -a /var/log/audit/audit.log
   ```

   The tool runs and generates a summary of error alerts and solutions. For example:

   ```
   SELinux is preventing /usr/sbin/sshd from write access on the sock_file /dev/log
   SELinux is preventing /usr/libexec/postfix/pickup from using the rlimitinh access on a process.
   ```

2. Execute the recommended solution for each error alert.

3. Restart Tenable.sc Director, as described in Start, Stop, or Restart Tenable.sc Director.
   
   Tenable.sc Director restarts.

4. Run the `sealert` tool again to confirm you resolved the error alerts.
Use /dev/random for Random Number Data Generation

**Required User Role:** Root user

If your organization requires Tenable.sc Director to use /dev/random instead of /dev/urandom to generate random number data for secure communication functions, modify the random data source using an environment variable.

Unlike /dev/urandom, /dev/random blocks HTTPS and SSL/TLS functions if there is not enough entropy to perform the functions. The functions resume after the system generates enough entropy.

**Note:** If /dev/random blocks during an installation or upgrade, the system waits up to 10 minutes for more entropy to be generated before halting the operation.

Tenable does not recommend using /dev/random unless required by your organization.

To use /dev/random for random number data generation in Tenable.sc Director:

1. Log in to Tenable.sc Director via the user interface.
2. Run the following command:

   ```bash
   export TSC_ENTROPY_CHECK=true
   ```

   Tenable.sc Director recognizes the environment variable and uses /dev/random.

What to do next:

- Install or upgrade Tenable.sc Director in order for your changes to take effect, as described in [Install Tenable.sc Director](#) or [Upgrade Tenable.sc Director](#).
License Requirements

Tenable.sc Director does not support an unlicensed demo mode. License keys are required for Tenable.sc Director and for all attached Tenable products. You first configure your Tenable.sc Director license and additional Tenable product licenses during quick start, as described in Quick Setup.

You can update your Tenable.sc Director license in an externally connected or air-gapped environment, as described in Update an Existing License.

Tenable.sc Director requires an internet connection to validate additional Tenable product licenses. To apply a license for an additional Tenable product, see Apply a New License. To update a license for an additional Tenable product, see Update an Existing License.

You cannot upgrade a Tenable.sc license to a Tenable.sc Director license or downgrade a Tenable.sc Director license to a Tenable.sc license.

Tip: For information about Tenable.sc-Tenable product registration server communications encryption, see Encryption Strength.

Your Tenable.sc License

Tenable.sc Director licenses are valid for a specific hostname and for a maximum number of active assets (identified by IP address or UUID). Assets are counted towards your license limit depending on how Tenable.sc discovers, or sees, the asset. In general, an asset does not count against your license limit unless it has been assessed for vulnerabilities.

For example, if you purchase a 500 asset Tenable.sc Director license, you can perform host discovery on your network but you cannot assess more than 500 assets. For more information about discovery and assessment scanning, see Scanning Overview.

Tenable.sc Director generates a warning in the web interface when you approach or exceed the license limit. To monitor your license limit, use the Licensing Status widget, as described in Overview Dashboard. To upgrade your license, contact your Tenable representative.

<table>
<thead>
<tr>
<th>Counted Toward License</th>
<th>Not Counted Toward License</th>
</tr>
</thead>
<tbody>
<tr>
<td>• IP addresses from active scans</td>
<td>• IP addresses present only from imports to offline repositories</td>
</tr>
<tr>
<td>• IP addresses from Log Correlation Engine instances</td>
<td>• IP addresses present only from NNM instances in discovery mode</td>
</tr>
</tbody>
</table>
Counted Toward License

- IP addresses from NNM instances not in discovery mode

A single IP address or UUID counts once toward your license, even if it was scanned by multiple methods or stored in multiple repositories.

**Note:** If you use an alternative port scanner, Tenable.sc Director counts the detected IP addresses against your license.

<table>
<thead>
<tr>
<th>Counted Toward License</th>
<th>Not Counted Toward License</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The following excluded plugins:</td>
</tr>
<tr>
<td></td>
<td><strong>Nessus</strong> — 10180, 10287, 10335, 11219, 11933, 11936, 12053, 14272, 14274, 19506, 22964, 33812, 33813, 34220, 34277, 45590, 54615, 87413, and 112154.</td>
</tr>
<tr>
<td></td>
<td><strong>NNM</strong> — 3, 12, 13, 18, 19, 20, 113, and 132.</td>
</tr>
<tr>
<td></td>
<td><strong>LCE</strong> — 800000 through 800099.</td>
</tr>
</tbody>
</table>

Your Tenable.sc Continuous View Product Licenses

If you want to use Tenable.sc Director with other Tenable products, you must add their activation codes to Tenable.sc. For more information, see [Apply a New License](#).
Apply a New License

**Required User Role:** Administrator

To apply a license for an additional Tenable product, add the license activation code. To update a license for an existing Tenable product, see [Update an Existing License](#).

For general information about licensing, see [License Requirements](#). For information about adding a license during quick setup, see [Quick Setup](#).

To apply a new Nessus, NNM, or LCE license:

1. Log in to Tenable.sc via the user interface.
2. Click **System > Configuration**.
   The **Configuration** page appears.
3. Click the **License** tile.
   The **License Configuration** page appears.
4. Click the product box for the license you want to apply.
5. In the box, type the activation code for the product.
6. Click **Register**.

   Tenable.sc updates the page to reflect the activation code status:
   - **Valid Code**: A green box with a check mark.
   - **Invalid Code**: A red box with an X.

   If the code is valid, Tenable.sc initiates a plugin download.
Update an Existing License

**Required User Role:** Administrator

If you need to replace your Tenable.sc Director license or the license activation code for your Nessus, Nessus Network Monitor, or Log Correlation Engine license, update the license.

To apply a new license for an additional Tenable product for the first time, see [Apply a New License](#).

You can update your Tenable.sc Director license in an externally connected or air-gapped environment. Tenable.sc Director requires an internet connection to validate product licenses for Nessus, NNM, or LCE.

For general information about licensing, see [License Requirements](#).

To update a license:

1. Log in to Tenable.sc Director via the user interface.
2. Click **System > Configuration**.
   
   The **Configuration** page appears.
3. Click the **License** tile.
   
   The **License Configuration** page appears.
4. To replace your Tenable.sc Director license, in the **Tenable.sc Director License** section:
   a. Click **Update License**.
   b. Click **Choose File** and browse to the license file you want to upload.
      
      Tenable.sc Director applies the new license.
5. To replace an activation code for an integrated product license, in the **Activation Codes** section:
   a. Click the green check mark.
   b. Click **Reset Activation Code**.
   c. In the box, paste your product license activation code.
   d. Click **Register**.
Tenable.sc Director communicates with the Tenable product registration server to validate your license activation code.

If the code is valid, Tenable.sc Director applies the new license and initiates a plugin download.
Tenable.sc Director License Expiration

This topic describes the behavior of Tenable.sc Director if you allow your software maintenance license to expire. Software maintenance licenses can be either perpetual or subscription-based.

**Tenable.sc Console**

- Perpetual license—The software remains fully functional. All user data is accessible. However, the Tenable.sc feed stops (that is, Tenable.sc Director no longer receives new plugin updates, dashboard updates, report updates, or audit file updates). Scan and data collection functionality is inhibited as described in the NNM, LCE, and Nessus sections below.

- Subscription license—You can no longer access the console unless you enter a new license key. Normal operation resumes once you replace the license key.

**Nessus**

When the software maintenance period expires, Nessus stops receiving plugin updates. After a period of 90 days, Nessus stops working and cannot perform new scans. Because Tenable.sc Director stops receiving feeds once the maintenance period expires, the Nessus scanners managed by your managed Tenable.sc instances no longer receive updates and stop working after the 90-day period.

**NNM**

After 30 days with no updates, NNM stops processing new data.

**LCE**

LCE stops processing new logs on the day of license expiration, but you can still query existing data within LCE.
Port Requirements

Your Tenable.sc Director deployment requires access to specific ports for inbound and outbound traffic.

Inbound Traffic

You must allow inbound traffic to the following ports.

<table>
<thead>
<tr>
<th>Port</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 22</td>
<td>Performing remote repository synchronization with another Tenable.sc.</td>
</tr>
<tr>
<td>TCP 443</td>
<td>Accessing the Tenable.sc Director interface.</td>
</tr>
</tbody>
</table>

Outbound Traffic

You must allow outbound traffic to the following ports.

<table>
<thead>
<tr>
<th>Port</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 25</td>
<td>Sending SMTP email notifications.</td>
</tr>
<tr>
<td>TCP 443</td>
<td>Communicating with Tenable.io.</td>
</tr>
<tr>
<td></td>
<td>Communicating with the plugins.nessus.org server for plugin updates.</td>
</tr>
<tr>
<td>TCP 1243</td>
<td>Communicating with Log Correlation Engine.</td>
</tr>
<tr>
<td>TCP 8834</td>
<td>Communicating with Nessus.</td>
</tr>
<tr>
<td>TCP 8835</td>
<td>Communicating with Nessus Network Monitor.</td>
</tr>
<tr>
<td>UDP 53</td>
<td>Performing DNS resolution.</td>
</tr>
</tbody>
</table>
Web Browser Requirements

You can access the Tenable.sc Director user interface using the following browsers:

- Microsoft Internet Explorer 10 or later
- Mozilla Firefox 32 or later
- Google Chrome 37 or later
- Mac OS Safari 7.1 or later
Tenable Integrated Product Compatibility

The release notes list the versions of Tenable products tested with Tenable.sc Director 5.17.x. For more information, see the Tenable.sc Release Notes for your version.
Large Enterprise Deployments

You may have a number of unique technical and business requirements to consider when planning a large enterprise deployment of Tenable.sc. If your organization scans 100,000 or more IP addresses, consider the information in the Tenable.sc Large Enterprise Deployment Guide when planning, configuring, and operationalizing your Tenable.sc deployment.
Installation and Upgrade

To perform a fresh installation of Tenable.sc Director, see Before You Install and Install Tenable.sc Director.

To perform an upgrade of Tenable.sc Director, see Before You Upgrade and Upgrade Tenable.sc Director.

To uninstall Tenable.sc Director, see Uninstall Tenable.sc Director.
Before You Install

**Note:** A basic understanding of Linux is assumed throughout the installation, upgrade, and removal processes.

Understand Tenable.sc and Tenable.sc Director Licenses

Confirm your licenses are valid for your Tenable.sc Director deployment. Tenable.sc Director does not support an unlicensed demo mode.

For more information, see [License Requirements](#).

Disable Default Web Servers

Tenable.sc Director provides its own Apache web server listening on port 443. If the installation target already has another web server or other service listening on port 443, you must disable that service on that port or configure Tenable.sc Director to use a different port after installation.

Identify which services, if any, are listening on port 443 by running the following command:

```
# ss -pan | grep ':443'
```

Modify Security Settings

Tenable.sc Director supports disabled, permissive, and enforcing mode Security-Enhanced Linux (SELinux) policy configurations. For more information, see [SELinux Requirements](#).

Perform Log File Rotation

The installation does not include a log rotate utility; however, the native Linux `logrotate` tool is supported post-installation. In most Red Hat environments, `logrotate` is installed by default. The following logs are rotated if the `logrotate` utility is installed:

- All files in `/opt/sc/support/logs` matching `*log`
- `/opt/sc/admin/logs/sc-error.log`

During an install/upgrade, the installer drops a file named `SecurityCenter` into `/etc/logrotate.d/` that contains log rotate rules for the files mentioned above.

Log files are rotated on a monthly basis. This file is owned by root/root.
Allow Tenable Sites

To allow Tenable.sc Director to communicate with Tenable servers for product updates and plugin updates, Tenable recommends adding Tenable sites to an allow list at the perimeter firewall. For more information, see the knowledge base article.
Install Tenable.sc Director

Required User Role: Root user

Note: A basic understanding of Linux is assumed throughout the installation, upgrade, and removal processes.

Caution: When performing sudo installs, use sudo –i to ensure the proper use of environmental variables.

Caution: During the installation process, Tenable.sc produces a log file in a temporary location: /tmp/sc.install.log. Once the installation process finishes, the file is stored here: /opt/sc/admin/logs/install.log. Do not remove or modify these files; they are important for debugging in case of a failed installation.

For information about new features, resolved issues, third-party product updates, and supported upgrade paths, see the release notes for Tenable.sc Director 5.17.x.

Before you begin:

- Complete system prerequisites, as described in Before You Install.
- Download the installation RPM file from the Tenable downloads page. If necessary, depending on the operating system of the host, move the installation RPM file onto the host.
- Confirm the integrity of the installation RPM file by comparing the download checksum with the checksum on the Tenable downloads page, as described in the knowledge base article.
- If your organization requires Tenable.sc to use /dev/random instead of /dev/urandom to generate random number data for secure communication functions, modify the random data source as described in Use /dev/random for Random Number Data Generation.

To install Tenable.sc Director:

1. On the host where you want to install Tenable.sc Director, open the command line interface (CLI).

2. Install the RPM by running one of the following commands:

   # rpm -ivh SecurityCenter-x.x.x-el6.x86_64.rpm
- or -

```
# rpm -ivh SecurityCenter-x.x.x-el7.x86_64.rpm
```

Output similar to the following is generated:

```
# rpm -ivh SecurityCenter-5.x.x-es6.x86_64.rpm
Preparing... ################################################################################ [100%]
1:SecurityCenter ################################################################################ [100%]
Installing Nessus plugins ... complete
Applying database updates ... complete.
By default, SecurityCenter will listen for HTTPS requests on ALL available interfaces. To complete your installation, please point your web browser to one of the following URL(s):
https://x.x.x.x
Starting SecurityCenter services
[ OK ] SecurityCenter services: [ OK ]
```

The system installs the package into /opt/sc and attempts to start all required daemons and web server services.

**Tip:** In rare cases, a system restart is required after installation in order to start all services. For more information, see [Start, Stop, or Restart Tenable.sc Director](#).
Quick Setup

The Tenable.sc Director Quick Setup Guide walks through the following configurations:

- License
- Connect Tenable.sc Instances
- Organization
- User

After configuring, Review and confirm.

License

Upload your Tenable.sc Director license.

Tenable.sc Director License

Click Choose File to upload the Tenable.sc Director license file you received from Tenable. The file should follow the format:

<CompanyName>_SC<IP Count>-<#>-<#>.key

After uploading and clicking the Activate button, the page confirms successful upload and activation of a valid license.

Activation Codes

Consider adding additional license activation codes:

- Tenable.sc license activation code — required before adding any Nessus scanners. The Tenable.sc license activation code allows Tenable.sc to download plugins and update Nessus scanner plugins.

  In the Nessus section, type the Tenable.sc activation code and click Register.

- NNM license activation code — required before using and managing attached NNM scanners.

  In the NNM section, type the NNM activation code and click Register.
• LCE Activation Code — required before downloading LCE Event vulnerability plugins to Tenable.sc. The LCE Activation Code allows Tenable.sc to download event plugins, but it does not manage plugin updates for LCE servers.

In the **LCE** section, type the Log Correlation Engine activation code and click **Register**.

Click **Next** to continue.

A plus (+) sign indicates that no license is applied for the product. A box with an X indicates an invalid activation code. Click on the plus (+) or X to add or reset a license activation code.

A box with a checkmark indicates a valid license is applied and that Tenable.sc initiated a plugin download in the background. The download may take several minutes and must complete before initiating any Nessus scans. After the download completes, the **Last Updated** date and time update on the Plugins page.

**Connect Tenable.sc Instances**

Connect the Tenable.sc instances you want to monitor from Tenable.sc Director. For information about the options you configure, see **Managed Tenable.sc Instance Settings**.

**Organization**

An organization is a set of distinct users and groups and the resources they have available to them. For information about the options you can configure, see **Organizations**.

You can configure one organization during initial setup. If you want to use multiple organizations, you must configure other organizations after the Quick Start.

**User**

You must create one administrator and one security manager during initial setup. For more information, see **User Roles**.

- Security manager — a user to manage the organization you just created. After you finish initial setup, the security manager can create other user accounts within the organization.

- Administrator — a user to manage Tenable.sc. After you finish initial setup, the administrator can create other organizations and user accounts.

After creating the security manager user and setting the administrator password, click **Next** to finish initial setup. The **Admin Dashboard** page appears, where you can review login configuration data.
Review

The review page displays your currently selected configurations. If you want to make further changes, click on the links in the left navigation bar.

When you are finished, click **Confirm**.
Before You Upgrade

**Note:** A basic understanding of Linux is assumed throughout the installation, upgrade, and removal processes.

- Tenable.sc Director Upgrade Path
- Java Version Requirements
- Halt or Complete Running Jobs
- Perform a Tenable.sc Director Backup
- Rename Your Mount Point

## Tenable.sc Director Upgrade Path

For more information about the upgrade paths to version 5.17.x, see the [Tenable.sc Release Notes](#).

## Java Version Requirements

If the Oracle Java JRE or OpenJDK is not installed, Tenable.sc Director displays the following warning:

> [WARNING] SecurityCenter has determined that Oracle Java JRE and OpenJDK is not installed. One of two must be installed for SecurityCenter reporting to function properly.

You must install the latest version of Oracle Java JRE or OpenJDK to take full advantage of Tenable.sc reporting.

## Halt or Complete Running Jobs

Tenable recommends stopping all running Tenable.sc Director processes before beginning an upgrade. If processes are running (e.g., Nessus scans), Tenable.sc displays the following message along with the related process names and their PIDs:

> SecurityCenter has determined that the following jobs are still running. Please wait a few minutes before performing the upgrade again. This will allow the running jobs to complete their tasks.

Stop the processes manually or retry the upgrade after the processes complete.
Perform a Tenable.sc Director Backup

Perform a backup of Tenable.sc Director before beginning your upgrade. For more information, see Backup and Restore.

Rename Your Mount Point

If the existing /opt/sc4 or /opt/sc directory is or contains a mount point to another location it must be updated. During the rpm upgrade process, a message appears with information about the discovered mount point and instructs you to contact Tenable Support for a mount point tool to help identify and migrate your mount points for the upgrade to continue.
Upgrade Tenable.sc Director

**Required User Role:** Root user

**Note:** This topic assumes a basic understanding of Linux.

**Caution:** During the upgrade process, Tenable.sc produces a log file in a temporary location: 
/tmp/sc.install.log. Once the installation process finishes, the file is stored here: 
/opt/sc/admin/logs/install.log. Do not remove or modify these files; they are important for debugging in case of a failed upgrade.

For information about new features, resolved issues, third-party product updates, and supported upgrade paths, see the release notes for Tenable.sc Director 5.17.x.

**Before you begin:**

- Complete system prerequisites, as described in Before You Upgrade.
- Download the upgrade RPM file from the Tenable downloads page. If necessary, depending on the operating system of the host, move the upgrade RPM file onto the host.
- Confirm the integrity of the upgrade RPM file by comparing the download checksum with the checksum on the Tenable downloads page.
- If your organization requires Tenable.sc to use /dev/random instead of /dev/urandom to generate random number data for secure communication functions, modify the random data source as described in Use /dev/random for Random Number Data Generation.

**To upgrade to Tenable.sc Director 5.17.x:**

1. Log in to Tenable.sc Director via the CLI.
2. Prepare the upgrade command you intend to run:
   - Use `rpm` with the “-Uvh” switches from the command-line of the Tenable.sc Director server.
   - Use “sudo -i” when performing sudo upgrades of Tenable.sc Director to ensure the proper use of environmental variables.

   For example:
The upgrade begins. Tenable.sc is not available until the upgrade finishes.

If custom Apache SSL certificates are in use prior to the upgrade, the Tenable.sc Director backs the certificates up as part of the upgrade process. Tenable.sc Director copies the existing custom SSL certificates to the Apache configuration backup directory that the upgrade process creates in the /tmp/[version].apache.conf-######## directory. The exact name of the directory varies, but the system displays the name during the upgrade process, as well as reports it in the /opt/sc/admin/log/install.log file.

To restore custom SSL certificates after upgrade:
1. Type the following command:

```
# cp /tmp/[version].apache.conf-########/SecurityCenter.cert
/opt/sc/support/conf/SecurityCenter.crt
```

2. Select yes to overwrite the existing file.

3. Type the following command:

```
# cp /tmp/[version].apache.conf-########/SecurityCenter.pem
/opt/sc/support/conf/SecurityCenter.key
```

4. Select yes to overwrite the existing file.

```
Caution: Ensure that the newly copied files have permissions of 0640 and ownership of tns:tns.
```

5. Modify the `servername` parameter in `/opt/sc/support/conf/servername` to match the Common Name (CN) of the SSL certificate.

```
Tip: To obtain the CN, run the following command and note the CN= portion of the result.

# /opt/sc/support/bin/openssl verify
/opt/sc/support/conf/SecurityCenter.crt
```

6. Restart the Apache server with one of the following commands:

```
# /opt/sc/support/bin/apachectl restart
```

-or-

```
# service SecurityCenter restart
```
Uninstall Tenable.sc Director

Required User Role: Root user

To uninstall Tenable.sc Director:

1. Log in to Tenable.sc Director via the CLI.

2. Stop Tenable.sc Director with the following command:

   ```
   service SecurityCenter stop
   ```

3. Determine the name of the RPM package with the following command:

   ```
   rpm -qa | grep SecurityCenter
   ```

   The name of the RPM package appears.

4. Remove the Tenable.sc Director package with one of the following commands:

   ```
   rpm -e SecurityCenter-x.x.x-el6.x86_64.rpm
   - or -
   ```

   ```
   rpm -e SecurityCenter-x.x.x-el7.x86_64.rpm
   ```

5. Remove user-created and user-modified files with the following command:

   ```
   rm -rf /opt/sc
   ```

Tenable.sc Director is removed.
User Access

The Users page provides the ability to add, edit, delete, or view the details of Tenable.sc Director user accounts. When you view the Users page, you see a list of users and actions, limited by your account privileges. Your user role, organization membership, and/or group membership determine your account privileges. For more information, see User Roles and Organizations and Groups.

There are two categories of user accounts:

- Administrator users have the system-provided administrator role and do not belong to organizations.

- Organizational users have the system-provided security manager, auditor, credential manager, executive, security analyst, security manager, or vulnerability analyst role, or a custom role, and belong to an organization.

Tenable.sc Director supports three types of user account authentication: TNS, LDAP, and SAML. For more information, see User Accounts.

To log in to the Tenable.sc Director web interface with a user account, see Log In to the Web Interface or Log in to the Web Interface via SSL Client Certificate.
Log In to the Web Interface

**Required User Role:** Any

To log in to the Tenable.sc Director configuration interface:

1. Open a supported web browser on a system that has access to the system’s network address space.

   **Note:** You must access the Tenable.sc Director web interface using a secure web connection (HTTPS) with SSL/TLS 1.2 enabled. Tenable.sc Director recommends configuring the strongest encryption supported by your browser.

   For more information, see [Encryption Strength](#).

2. Clear your web browser’s cache.

3. Navigate to the URL for your Tenable.sc Director: `https://<SERVER ADDRESS OR NAME>/`.

   Where `<SERVER ADDRESS OR NAME>` is the IPv4 or IPv6 address or hostname for your Tenable.sc Director.

   The Tenable.sc Director web interface appears.

4. Log in using the supported method for your account configuration.

   **Note:** If you are the first administrator user logging in to Tenable.sc Director, see [Initial Login Considerations](#).

   - To log in via a username and password, type your Tenable.sc Director credentials and click **Log In**.
   - To log in via SAML authentication, click **Sign In Using Identity Provider**. When presented with your identity provider login page, type your identity provider credentials.
     
     For more information about SAML authentication, see [Configure SAML Authentication Manually via the User Interface](#).
   - To log in via certificate, see [Log in to the Web Interface via SSL Client Certificate](#).

Tenable.sc Director logs you in and displays the dashboard with different elements depending on your user role.
Initial Login Considerations

When you log in to Tenable.sc Director for the first time, Tenable.sc Director displays the Quick Setup Guide welcome page to begin a multi-step setup process for initial configuration. For more information about quick setup, see Quick Setup.

If you prefer to configure the system manually, click Exit Quick Setup Guide. For more information about getting started with Tenable.sc Director, see Get Started With Tenable.sc Director.
Log in to the Web Interface via SSL Client Certificate

Required User Role: Any

Before you begin:

- Confirm your Tenable.sc Director administrator fully configured Tenable.sc Director for certificate authentication, as described in Certificate Authentication.

To perform a certificate-based Tenable.sc Director login:

Note: The following information is provided with the understanding that your browser is configured for SSL certificate authentication. Please refer to your browser’s help files or other documentation to configure this feature.

1. Open a browser window and navigate to Tenable.sc Director.
   The browser presents a list of available certificate identities.
   For information about Tenable.sc Director-browser communications encryption, see Encryption Strength.

2. Select a certificate.
3. Click **OK**.

   An authentication prompt appears (if required to access your certificate).

4. (Optional) If prompted, type a PIN or password.

5. Click **OK**.

   The Tenable.sc Director login page appears.

6. Log in using the username to be associated with the selected certificate.

   ![Certificate Authentication Window](image)

   **Caution:** Only one Tenable.sc Director user may be associated with a single certificate. If one user holds multiple user names and roles, a unique certificate must be provided for each login name.

   The **Certificate Authentication** window appears.

7. When prompted, specify whether the current certificate is to be used to authenticate the current user.

   - Click **Yes** to always use the certificate for authentication.
   - Click **No** to ignore the certificate and log in via TNS authentication.

   Tenable.sc logs you in.

**Subsequent Logins**

After you log out of Tenable.sc Director, Tenable.sc Director displays the login page. If you want to log in again with the same certificate, refresh your browser window. If you want to use a different certificate, you must start a new browser session.
After you perform your second certificate login, edit your account from the **Profile** page to view your certificate details. If your certificate changes or you need to revoke it, click the **Clear Certification Details** button to disassociate the certificate from your account.
User Roles

Roles determine what a user can or cannot access from their account. Tenable.sc Director comes with eight system-provided roles, but you can also create custom roles to satisfy complex security policy needs. You can customize the permissions on some, but not all, system-provided user roles.

If you configure linked user accounts, an Administrator can switch to one or more Security Manager user accounts without logging out and logging back in to Tenable.sc Director. For more information, see Linked User Accounts.

For more information about user roles in Tenable.sc Director, see Create a User Role, Edit a User Role, and Delete a User Role.

<table>
<thead>
<tr>
<th>User Role</th>
<th>Customizable Permissions?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>No</td>
<td>An account that manages Tenable.sc Director as a whole. The primary task of the Administrator is to install and configure each organization and connect managed Tenable.sc instances. The Administrator is automatically assigned the “Manage Application” role. Because administrators do not belong to an organization, they do not have access to the data collected by Tenable.sc Director.</td>
</tr>
</tbody>
</table>

Organizational User Roles

<table>
<thead>
<tr>
<th>User Role</th>
<th>Customizable Permissions?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Manager</td>
<td>No</td>
<td>An account that manages an individual organization. This is the role assigned to the initial user that is assigned when a new organization is created. They have the ability to launch scans, configure users (except for administrator user roles), vulnerability policies, and other objects belonging to their organization. A Security Manager is the account within an organization that has a broad range of security roles within the defined organization. This is the initial user that is created when a new organization is created and has the ability to launch scans, configure users (except for the Administrator user), vulnerability policies, and other objects that belong to their organization. This initial</td>
</tr>
</tbody>
</table>
Security Manager account cannot be deleted without deleting the entire organization.

Security Managers have complete access to all data collected by their organization.

<table>
<thead>
<tr>
<th>Role</th>
<th>Yes/No</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditor</td>
<td>Yes</td>
<td>An account that can access summary information to perform third party audits. An Auditor can view dashboards, reports, and logs, but cannot perform scans or analyze vulnerability or event data.</td>
</tr>
<tr>
<td>Credential Manager</td>
<td>Yes</td>
<td>An account that can be used specifically for handling credentials. A Credential Manager can create and share credentials without revealing the contents of the credential. This can be used by someone outside the security team to keep scanning credentials up to date.</td>
</tr>
<tr>
<td>Executive</td>
<td>Yes</td>
<td>An account intended for users who are interested in a high-level overview of their security posture and risk profile. Executives would most likely browse dashboards and review reports, but would not be concerned with monitoring running scans or managing users. Executives would also be able to assign tasks to other users using the ticketing interface.</td>
</tr>
<tr>
<td>Security Analyst</td>
<td>Yes</td>
<td>An account that has permissions to perform all actions at the Organizational level except managing groups and users. A Security Analyst is most likely an advanced user who can be trusted with some system related tasks such as setting black-out windows or updating plugins.</td>
</tr>
<tr>
<td>Vulnerability Analyst</td>
<td>Yes</td>
<td>An account that can perform basic tasks within the application. A Vulnerability Analyst is allowed to view security data, perform scans, share objects, view logs, and work with tickets.</td>
</tr>
<tr>
<td>No Role</td>
<td>No</td>
<td>An account with virtually no permissions. No Role is assigned to a user if their designated role is deleted.</td>
</tr>
<tr>
<td>Custom Role</td>
<td>Yes</td>
<td>A custom role that you create by enabling or disabling individual permissions.</td>
</tr>
</tbody>
</table>

See the following table for more information about other user role options.
<table>
<thead>
<tr>
<th>Permissions Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Custom role name</td>
</tr>
<tr>
<td>Description</td>
<td>Custom role description</td>
</tr>
<tr>
<td><strong>Scan Permissions</strong></td>
<td></td>
</tr>
<tr>
<td>Create Scans</td>
<td>Allows the user to create policy-based scans. Disabling <strong>Create Policies</strong> while enabling this permission allows you to lock user into specific set of policies for scanning.</td>
</tr>
<tr>
<td>Create Agent Synchronization Jobs</td>
<td>Allows the user to add agent synchronization jobs that fetch agent scan results from Tenable.io or Nessus Manager.</td>
</tr>
<tr>
<td>Create Agent Scans</td>
<td>Allows the user to add agent scans that create and launch parallel scans in Nessus Manager, then import the scan results to Tenable.sc.</td>
</tr>
<tr>
<td>Create Audit Files</td>
<td>Allows the user to upload audit files, which can be used for configuration audit scans.</td>
</tr>
<tr>
<td>Create Policies</td>
<td>Allows the user to set scan parameters and select plugins for scanning.</td>
</tr>
<tr>
<td>Upload Nessus Scan Results</td>
<td>Allows the user to import results from an external Nessus scanner. Result upload will be limited to user’s repositories and restricted by user’s IP address ranges.</td>
</tr>
<tr>
<td>Manage Blackout Windows</td>
<td>Allows the user to add, edit, and delete organization-wide blackout windows. Blackout windows prevent scans from launching and stop any scans in progress.</td>
</tr>
<tr>
<td><strong>Asset Permissions</strong></td>
<td></td>
</tr>
<tr>
<td>Create LDAP Query Assets</td>
<td>Allows the user to create LDAP Query Assets, which update a list of hosts based on a user-defined LDAP query.</td>
</tr>
<tr>
<td><strong>Analysis Permissions</strong></td>
<td></td>
</tr>
<tr>
<td>Accept Risks</td>
<td>Allows the user to accept risks for vulnerabilities, which removes them from the default view for analysis, dashboards, and reports.</td>
</tr>
<tr>
<td>Permissions Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Recast Risks</td>
<td>Allows the user to change the severity for vulnerabilities.</td>
</tr>
<tr>
<td><strong>Organizational Permissions</strong></td>
<td></td>
</tr>
<tr>
<td>Share Objects Between Groups</td>
<td>Allows the user to share assets, audit files, credentials, queries, and policies with any group. Users in groups to which these objects have been shared will be able to use them for filtering and scan creation.</td>
</tr>
<tr>
<td>View Organization Logs</td>
<td>Allows the user to view logs for entire organization.</td>
</tr>
<tr>
<td><strong>User Permissions</strong></td>
<td></td>
</tr>
<tr>
<td>Manage Roles</td>
<td>Allows the user to create new roles and edit and delete organizational roles. Any roles added must have permissions equal to or lesser than the user’s role.</td>
</tr>
<tr>
<td>Manage Groups</td>
<td>Allows the user to add, edit, and delete groups. Users with this permission are allowed to create groups with access to any vulnerability and event data available to the organization.</td>
</tr>
<tr>
<td>Manage Group Relationships</td>
<td>Allows the user to set other user’s relationship with any other groups. Group relationships allow for a user to view and manage objects and users in other groups.</td>
</tr>
<tr>
<td><strong>Report Permissions</strong></td>
<td></td>
</tr>
<tr>
<td>Manage Images</td>
<td>Allows the user to upload images, which can be used in reports by anyone in the organization.</td>
</tr>
<tr>
<td>Manage Attribute Sets</td>
<td>Allows the user to add, edit, and delete attribute sets.</td>
</tr>
<tr>
<td><strong>System Permissions</strong></td>
<td></td>
</tr>
<tr>
<td>Update Feeds</td>
<td>Allows the user to request a plugin update or a Tenable.sc feed update.</td>
</tr>
<tr>
<td><strong>Workflow Permissions</strong></td>
<td></td>
</tr>
<tr>
<td>Create Alerts</td>
<td>Allows the user to create alerts which are used to trigger actions (e.g., launch scans, run reports, send emails) when specified vulnerability or event conditions occur.</td>
</tr>
<tr>
<td>Permissions Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Create Tickets</td>
<td>Allows the user to create tickets, which are typically used to delegate work to other users.</td>
</tr>
</tbody>
</table>
Create a User Role

**Required User Role:** Administrator or organizational user with appropriate permissions. For more information, see [User Roles](#).

For more information about user role options, see [User Roles](#).

To create a custom user role:

1. Log in to Tenable.sc Director via the user interface.
2. Do one of the following:
   - If you are logged in as an administrator, click **System > Roles**.
   - If you are logged in as an organizational user, click **Users > Roles**.
   
   The **Roles** page appears.
3. Click **Add**.
4. In the **Name** box, type a name for the role.
5. (Optional) In the **Description** box, type a description for the role.
6. Set the **Scanning Permissions**, **Asset Permissions**, **Analysis Permissions**, **Organization Permissions**, **User Permissions**, **Reporting Permissions**, **System Permissions**, and **Workflow Permissions**.
7. Click **Submit**.

   Tenable.sc Director saves your configuration.
Edit a User Role

**Required User Role:** Administrator or organizational user with appropriate permissions. For more information, see [User Roles](#).

For more information about user role options, see [User Roles](#).

To edit the permissions of a custom or system-provided role:

1. Log in to Tenable.sc Director via the user interface.
2. Do one of the following:
   - If you are logged in as an administrator, click **System > Roles**.
   - If you are logged in as an organizational user, click **Users > Roles**.
   
   The **Roles** page appears.
3. In the row for the role you want to edit, click the menu.
   
   The actions menu appears.
4. Click **Edit**.
   
   The **Edit Role** page appears.
5. (Optional) Modify the **Name**
6. (Optional) Modify the **Description**.
7. (Optional) Modify the following permissions, as described in [User Roles](#)
   
   - **Scanning Permissions**
   - **Asset Permissions**
   - **Analysis Permissions**
   - **Organization Permissions**
   - **User Permissions**
   - **Reporting Permissions**
• System Permissions
• Workflow Permissions

8. Click **Submit**.

Tenable.sc Director saves your configuration.
Delete a User Role

**Required User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

For more information, see User Roles.

To delete a custom or system-provided user role:

**Note:** Deleting a role will cause all users with that role to lose all assigned permissions.

1. Log in to Tenable.sc Director via the user interface.

2. Do one of the following:
   - If you are logged in as an administrator, click System > Roles.
   - If you are logged in as an organizational user, click Users > Roles.

   The Roles page appears.

3. In the row for the role you want to delete, click the 🗿 menu.

   The actions menu appears.

4. Click Delete.

   A confirmation window appears.

5. Click Delete.

   Tenable.sc Director deletes the role.
Organizations and Groups

An organization is a set of distinct users and groups and the resources they have available to them. These users are assigned repositories and zones within one or more specified IP address networks. Users refers to any non-administrator user account on Tenable.sc Director. Groups refers to collections of users with the same permissions within an organization.

For more information, see Organizations and Groups.
Organizations

An organization is a set of distinct users and groups and the resources (e.g., scanners, repositories, and LDAP servers) they have available to them.

The organization is managed primarily by the administrator users and security manager users. The administrator user creates the organization and creates, assigns, and maintains the security manager user account. The security manager user (or any organizational user with appropriate permissions) creates other users within the organization. Groups allow you to manage users and share permissions to resources and objects among the group. For more information, see User Access.

Multiple organizations can share the same repositories, and the vulnerability data associated with the overlapping ranges is shared between each organization. Conversely, organizations can be configured with their own discrete repositories to facilitate situations where data must be kept confidential between different organizational units.

Creation of an organization is a multi-step process. After you create an organization, Tenable.sc Director prompts you to create the initial security manager user. For more information, see Add an Organization and Delete an Organization.

To view details for any organization, see View Organization Details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>(Required) The organization name.</td>
</tr>
<tr>
<td>Description</td>
<td>A description for the organization.</td>
</tr>
<tr>
<td>Contact Information</td>
<td>The relevant contact information for the organization including address,</td>
</tr>
<tr>
<td></td>
<td>city, state, country, and phone number.</td>
</tr>
<tr>
<td>Scanning</td>
<td></td>
</tr>
<tr>
<td>Distribution Method</td>
<td>The scan distribution mode you want to use for this organization:</td>
</tr>
<tr>
<td></td>
<td>• Automatic Distribution Only: Tenable.sc chooses one or more scan zones</td>
</tr>
<tr>
<td></td>
<td>to run the scan. Organizational users cannot choose a scan zone when</td>
</tr>
<tr>
<td></td>
<td>configuring a scan.</td>
</tr>
<tr>
<td></td>
<td>Tenable.sc distributes targets for scans based on your configured scan</td>
</tr>
<tr>
<td></td>
<td>zone ranges. This facilitates optimal scanning</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>and is very useful if an organization has devices placed behind a firewall or NAT device or has conflicting <a href="https://tools.ietf.org/html/rfc1918">RFC 1918</a> non-internet-routable address spaces.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Locked Zone:</strong> Tenable.sc uses the one <strong>Available Zone</strong> you specify to run the scan. Organizational users cannot modify the scan zone when configuring a scan.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Selectable Zones:</strong> Tenable.sc allows organizational users to select a scan zone when configuring a scan.</td>
</tr>
<tr>
<td></td>
<td>This mode allows organizational users to use scanners to run internal and external vulnerability scans and analyze the vulnerability stance from a new perspective. For example, an organizational user can choose an external scanner to see the attack surface from an external attacker’s perspective.</td>
</tr>
<tr>
<td></td>
<td>For more information about scan zones, see <a href="#">Scan Zones</a>.</td>
</tr>
<tr>
<td>Available Zones</td>
<td>One or more scan zones that you want organizational users to have access to when configuring scans.</td>
</tr>
<tr>
<td>Allow for Automatic Distribution</td>
<td>Enable or disable this option to specify whether you want Tenable.sc to automatically select one or more scan zones if an organizational user does not specify a scan zone when configuring a scan.</td>
</tr>
<tr>
<td></td>
<td>• When enabled, Tenable.sc chooses one or more scan zones as specified by your <strong>Restrict to Selected Zones</strong> setting.</td>
</tr>
<tr>
<td></td>
<td>• When disabled, Tenable.sc requires the organizational user to specify a scan zone when configuring a scan.</td>
</tr>
<tr>
<td>Restrict to Selected Zones</td>
<td>If <strong>Allow for Automatic Distribution</strong> is enabled, enable or disable this option to specify the zones you want Tenable.sc to choose from when automatically distributing zones.</td>
</tr>
<tr>
<td></td>
<td>• When enabled, Tenable.sc chooses from the <strong>Available Zones</strong> shared with the organization.</td>
</tr>
<tr>
<td></td>
<td>• When disabled, Tenable.sc chooses from all zones on Tenable.sc.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>able.sc.</td>
<td></td>
</tr>
<tr>
<td>Restricted Scan Ranges</td>
<td>The IP address ranges you do not want users in this organization to scan.</td>
</tr>
<tr>
<td>Analysis</td>
<td></td>
</tr>
<tr>
<td>Accessible LCEs</td>
<td>The LCEs that you want this organization to have access to. You can search for the LCEs by name or scroll through the list.</td>
</tr>
<tr>
<td>Accessible Repositories</td>
<td>The repositories that you want this organization to have access to. You can search for the repositories by name or scroll through the list.</td>
</tr>
<tr>
<td>Accessible Agent Capable Scanners</td>
<td>The Nessus scanners (with Nessus Agents enabled) that you want this organization to have access to. Select one or more of the available scanners to allow the organization to import Nessus Agent results from the selected scanner.</td>
</tr>
<tr>
<td>Accessible LDAP Servers</td>
<td>The LDAP servers that you want this organization to have access to. An organization must have access to an LDAP server in order to perform LDAP authentication on user accounts within that organization, and to configure LDAP query assets.</td>
</tr>
</tbody>
</table>

**Note:** If you revoke access to an LDAP server, users in the organization cannot authenticate and LDAP query assets cannot run.

### Custom Analysis Links

A list of custom analysis links provided to users within the host vulnerability details when analyzing data outside of Tenable.sc is desired. Click **Add Custom Link** to create a new option to type the link name and URL to look up additional data external to Tenable.sc.

For example: `http://example.com/index.htm?ip=%ip%`

The `%ip%` reference is a variable that inserts the IP address of the current host into the specified URI.

### Vulnerability Weights

<p>| Low                                         | The vulnerability weighting to apply to <strong>Low</strong> criticality vulnerabilities |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>The vulnerability weighting to apply to <strong>Medium</strong> criticality vulnerabilities for scoring purposes. (Default: 3)</td>
</tr>
<tr>
<td>High</td>
<td>The vulnerability weighting to apply to <strong>High</strong> criticality vulnerabilities for scoring purposes. (Default: 10)</td>
</tr>
<tr>
<td>Critical</td>
<td>The vulnerability weighting to apply to <strong>Critical</strong> criticality vulnerabilities for scoring purposes. (Default: 40)</td>
</tr>
</tbody>
</table>

**Vulnerability Scoring System**

| Scoring System | The scoring system Tenable.sc Director uses to assess the severity of vulnerabilities: CVSS v2 or CVSS v3. |

**Note:** Changing the **Scoring System** while Tenable.sc Director is running certain operations, such as preparing reports or dashboard data, results in data using mixed CVSS v2 and CVSS v3 scores.

**Note:** Changing the **Scoring System** does not impact historical dashboard trend data. For example, if you change the **Scoring System** from CVSS v2 to CVSS v3, dashboard trend data prior to the change displays CVSS v2 scores and dashboard trend data after the change displays CVSS v3 scores.
Add an Organization

**Required User Role:** Administrator

For more information about organization options, see Organizations.

To add an organization:

1. Log in to Tenable.sc via the user interface.
2. Click System > Organizations.
   
   The Organizations page appears.
3. Click Add.
   
   The Add Organization page appears.
4. Configure the following settings:
   
   - General
   - Scanning
   - Analysis
   - Custom Analysis Links
   - Vulnerability Weights
   - Vulnerability Scoring System
5. Click Submit.
   
   Tenable.sc Director saves your configuration.
View Organization Details

Required User Role: Administrator

You can view details for any organization. For more information, see Organizations.

To view organization details:

1. Log in to Tenable.sc Director via the user interface.
2. Click System > Organizations.
   The Organizations page appears.
3. In the row for the organization, click the menu.
   The actions menu appears.
4. Click View.
   The View Organization page appears.

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>View general information for the organization.</td>
</tr>
<tr>
<td></td>
<td>• Name — The organization name.</td>
</tr>
<tr>
<td></td>
<td>• Description — The organization description.</td>
</tr>
<tr>
<td></td>
<td>• Address / City / State / Country / Phone — The contact information for the organization.</td>
</tr>
<tr>
<td></td>
<td>• Created — The date the organization was created.</td>
</tr>
<tr>
<td></td>
<td>• Last Modified — The date the organization was last modified.</td>
</tr>
<tr>
<td></td>
<td>• ID — The organization ID.</td>
</tr>
<tr>
<td>Scanning</td>
<td>View a summary of your scanning settings for the organization. For more information about a setting, see Organizations.</td>
</tr>
<tr>
<td>Analysis</td>
<td>View a summary of your analysis settings for the organization. For more information about a setting, see Organizations.</td>
</tr>
<tr>
<td>Section</td>
<td>Action</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Custom Analysis Links</td>
<td>View a summary of your custom analysis link settings for the organization. For more information about a setting, see <a href="#">Organizations</a>.</td>
</tr>
<tr>
<td>Vulnerability Weights</td>
<td>View a summary of your vulnerability weights settings for the organization. For more information about a setting, see <a href="#">Organizations</a>.</td>
</tr>
</tbody>
</table>
Delete an Organization

**Required User Role:** Administrator

For more information, see [Organizations](#).

To delete an organization:

**Note:** Deleting an organization deletes all of the users in that organization.

1. Log in to Tenable.sc Director via the user interface.

2. Click **System > Organizations**.
   - The **Organizations** page appears.

3. In the row for the organization you want to delete, click the **⋯** menu.
   - The actions menu appears.

4. Click **Delete**.
   - A confirmation window appears.

5. Click **Delete**.
   - Tenable.sc Director deletes the organization.
Groups

User groups are a way to group rights to objects within an organization, and then quickly assign these rights to one or more users. A user's group membership determines their access to security data. When a user creates various objects such as reports, scan policies, dashboards, and other similar items, these objects are automatically shared among the group members if the group permissions allow view and control.

The following table describes the options to configure a group.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General tab</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The name for the group.</td>
</tr>
<tr>
<td>Description</td>
<td>A description for the group (e.g., security team at the central office or executives on the east coast).</td>
</tr>
<tr>
<td>Viewable Hosts</td>
<td>The IP addresses and agent IDs that are viewable by the group. The selection is made by all defined assets or the selection of one or more asset lists.</td>
</tr>
<tr>
<td>Repositories</td>
<td>The repositories you want to share with the group.</td>
</tr>
<tr>
<td>LCEs</td>
<td>The LCEs you want to assign to the group.</td>
</tr>
<tr>
<td>Sample Content</td>
<td>When enabled, Tenable provides sample content objects to users in the group:</td>
</tr>
<tr>
<td></td>
<td>• sample dashboards <em>(Executive 7 Day, Executive Summary, and Vulnerability Overview)</em></td>
</tr>
<tr>
<td></td>
<td>• sample reports <em>(Critical and Exploitable Vulnerabilities, Monthly Executive, and Remediation Instructions by Host)</em></td>
</tr>
<tr>
<td></td>
<td>• sample ARCs <em>(CCC 1: Maintain an Inventory of Software and Hardware, CCC 2: Remove Vulnerabilities and Misconfigurations, CCC 3: Deploy a Secure Network, CCC 4: Authorize Users, and CCC 5: Search for Malware and Intruders)</em></td>
</tr>
<tr>
<td></td>
<td>• sample assets required for the sample ARCs</td>
</tr>
<tr>
<td></td>
<td>After enabling Sample Content, you must add a new user to the group before all users in the group can access the sample content.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Note:</td>
<td>If a user in a group deletes a sample content object, the object is deleted for all other users in that group.</td>
</tr>
<tr>
<td>Note:</td>
<td>If you move a sample content object owner (e.g., move the first user in group A to group B), Tenable.sc: 1. Assigns their dashboards and ARCs to a new sample content object owner in group A. Tenable.sc does not reassign reports or assets. 2. Recreates their dashboards, ARCs, and assets required for ARCs in group B. Tenable.sc does not recreate reports.</td>
</tr>
</tbody>
</table>

**Share to Group tab**

| Available Objects | The list of available objects to be shared with the group on creation or edit in a bulk operation. |

For more information, see Add a Group and Delete a Group.
Add a Group

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

For more information about group options, see [Groups](#).

To add a group:

1. Log in to Tenable.sc via the user interface.
2. Click **Users > Groups**.
3. Click **Add**.
4. Configure the **General** options.
5. Configure the **Share to Group** options.
6. Click **Submit**.

   Tenable.sc Director saves your configuration.
Delete a Group

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

To delete a group:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Users > Groups**.
3. In the row for the group you want to delete, click the ⌁ menu.
   
   The actions menu appears.
4. Click **Delete**.
   
   A confirmation window appears.
5. Click **Delete**.
   
   Tenable.sc Director deletes the group.
User Accounts

The Users page displays the user accounts on Tenable.sc Director, limited by your account privileges. You can sort the columns or apply filters to locate specific user accounts. You can also add a user (Add a TNS-Authenticated User, Add an LDAP-Authenticated User, or Add a SAML-Authenticated User) or Delete a User.

You can create one or more administrator accounts on Tenable.sc Director. You can create one or more organizational users (security managers and/or custom roles) per organization. Tenable recommends you make at least one TNS-authenticated administrator and security manager user per organization. If the LDAP or SAML service becomes unavailable, you can still log in.

Linked User Accounts

You can create linked user accounts to allow an Administrator user to switch to one or more Security Manager accounts without logging out and logging back in to Tenable.sc Director. For more information, see Linked User Accounts.

API Keys

You can generate API keys to authenticate as a specific user for Tenable.sc API requests. For more information, see API Key Authentication.

User Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Authentication Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>All</td>
<td>The role assigned to the user. For more information, see User Roles. Administrator users can create Administrator or Security Manager user accounts. Organizational users can create Auditor, Credential Manager, Executive, No Role, Security Analyst, Security Manager, or Vulnerability Analyst accounts at their own privilege level or lower. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- If a user is an Auditor, they can create new Auditors or</td>
</tr>
<tr>
<td>Option</td>
<td>Authentication Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Organization</td>
<td>All</td>
<td>The organization where you want to assign the user account.</td>
</tr>
<tr>
<td>First Name / Last Name</td>
<td>All</td>
<td>(Optional) The given first name and last name for the user.</td>
</tr>
<tr>
<td>Type</td>
<td>All</td>
<td>The type of authentication you want to perform on the user:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Tenable (TNS)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Lightweight Directory Access Protocol (LDAP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Security Assertion Markup Language (SAML)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You must configure an LDAP server or SAML authentication in order to see LDAP or SAML in the Type drop-down box.</td>
</tr>
<tr>
<td>Username / Password</td>
<td>TNS</td>
<td>The username and password for the user account.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When selecting a username, it is sometimes easier to focus on the person’s real name as a convention (e.g., Bob Smith would become bsmith). However, it may also be useful to assign names based on role, such as auditNY.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The username value is case-sensitive.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Tip:</strong> Tenable recommends using passwords that meet stringent length and complexity requirements.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For information about Tenable.sc Director password data encryption, see <a href="#">Encryption Strength</a>.</td>
</tr>
<tr>
<td>Username</td>
<td>SAML</td>
<td>The user’s SAML username. Type the username exactly as it appears in your identity provider SAML configuration for this role.</td>
</tr>
<tr>
<td>Option</td>
<td>Authentication Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Must Change Password</td>
<td>TNS</td>
<td>When enabled, the user must change their password upon initial login.</td>
</tr>
<tr>
<td>LDAP Server</td>
<td>LDAP</td>
<td>The server you want to use to authenticate the user.</td>
</tr>
</tbody>
</table>
| Search String                 | LDAP                | The LDAP search string you want to use to filter your user search. Use the format: `attribute=<filter text>`. You can use wildcards, and the option accepts up to 1024 characters. **Examples**
<p>|                               |                     | sAMAccountName=*                                                           |
|                               |                     | mail=a*                                                                    |
|                               |                     | displayName=C*                                                             |
| LDAP Users Found              | LDAP                | A filtered list of LDAP user accounts retrieved by the <strong>Search String</strong>. Your selection in this option populates the <strong>Username</strong> option. |
| Username                      | LDAP                | The username, populated by your <strong>LDAP Users Found</strong> selection. This username must match a user on the LDAP server in order to authenticate successfully. |
| Time Zone                     | All                 | The time zone for the user.                                                |
| Scan Result Default Time-frame| All                 | The default <strong>Completion Time</strong> filter applied when the user accesses or refreshes the scan results page. |
| Cached Fetching               | All                 | (Optional) When enabled, Tenable.sc Director caches plugin policy information and performs plugin policy downloads once per page load. |
| Group                          | All                 | The group where you want to assign the user account. A user's group determines their access to Tenable.sc Director resources. For more information about groups, see <strong>Groups</strong>. |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Authentication Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>All</td>
<td>(Optional) Assigns a user to an asset list for which the user is responsible. Assigning a user to an asset list makes it easier to determine who in a group or organization should be assigned tickets, notifications, and other tasks to resolve particular issues. Selecting an asset updates the User Responsibility Summary in the Vulnerability Analysis section.</td>
</tr>
<tr>
<td>Contact Information</td>
<td>All</td>
<td>(Optional) The contact information for the user.</td>
</tr>
</tbody>
</table>
Add a TNS-Authenticated User

**Required User Role:** Administrator or organizational user with appropriate permissions. For more information, see [User Roles](#).

For more information about user account configuration options, see [User Accounts](#).

To add a TNS-authenticated user account as an administrator user:

1. Log in to Tenable.sc via the user interface.
2. Click **System > Users**.
   - The **Users** page appears.
3. Click **Add**.
   - The **Add User** page appears.
4. Select a **Role**.
5. If you selected **Security Manager** as the **Role**, select an **Organization**.
6. (Optional) Type a **First Name** and **Last Name**.
7. Type a **Username** and **Password** for the user.
8. If the **Type** drop-down box is visible, select **TNS**.
9. (Optional) Enable **User Must Change Password**.
10. Select a **Time Zone**.
11. (Optional) Select a **Scan Result Default Timeframe**.
12. (Optional) Enable **Cached Fetching**.
13. (Optional) Type **Contact Information** for the user.
14. Click **Submit**.
   - Tenable.sc Director saves your configuration.

To add a TNS-authenticated user account as an organizational user:
1. Log in to Tenable.sc via the user interface. You must log in with a user account belonging to the organization where you want to create a new user.

2. Click **Users** > **Users**.

   The **Users** page appears.

3. Click **Add**.

   The **Add User** page appears.

4. (Optional) Type a **First Name** and **Last Name** for the user.

5. If the **Type** drop-down box is visible, select **TNS**.

6. Type a **Username** and **Password** for the user.

7. (Optional) Enable **User Must Change Password**.

8. Select a **Time Zone**.

9. (Optional) Select a **Scan Result Default Timeframe**.

10. (Optional) Enable **Cached Fetching**.

11. Select a **Role**. For more information, see **User Roles**.

12. Select a **Group**. For more information, see **Organizations and Groups**.

13. (Optional) If you want to customize the group-related permissions for the user, modify the **Group Permissions** as described in **Custom Group Permissions**.

14. (Optional) If you want to share an asset list with the user, select an **Asset**. For more information, see **Assets**.

15. (Optional) Type **Contact Information** for the user.

16. Click **Submit**.

   Tenable.sc Director saves your configuration.
Add an LDAP-Authenticated User

**Required User Role:** Administrator or organizational user with appropriate permissions. For more information, see [User Roles](#).

For more information about user account configuration options, see [User Accounts](#).

To add an LDAP-authenticated user account as an administrator user:

1. Log in to Tenable.sc via the user interface.
2. Configure an LDAP server, as described in [LDAP Authentication](#). If you want the new user to be a member of an organization, associate the LDAP server with an organization.
3. Click **System > Users**.
   
   The **Users** page appears.
4. Click **Add**.
   
   The **Add User** page appears.
5. Select a **Role** for the user account.
6. If you selected **Security Manager** as the **Role**, select an **Organization** for the user account. You must select an organization with an associated LDAP server.
7. (Optional) Type a **First Name** and **Last Name** for the user.
8. In the **Type** drop-down list, select **LDAP**. If **LDAP** does not appear in the drop-down list, add an LDAP server as described in [Add an LDAP Server](#).
9. Select the **LDAP Server** where you want to authenticate the user.
10. Type a **Search String** to find existing users on the LDAP server.
11. Click **Search**.
    
    The page displays the **LDAP Users Found** by the LDAP search string.
12. Select an LDAP user from the **LDAP Users Found** drop-down box.
    
    The page populates the **Username** option with your selection.
13. View the **Username**. Tenable does not recommend modifying the **Username** since it must match the username on the LDAP server.

14. Select a **Time Zone**.

15. (Optional) Select a **Scan Result Default Timeframe**.

16. (Optional) Enable **Cached Fetching**.

17. (Optional) Type **Contact Information** for the user.

18. Click **Submit**.

   Tenable.sc Director saves your configuration.

To add an LDAP-authenticated user account as an organizational user:

1. Log in to Tenable.sc via the user interface. You must log in with a user account belonging to the organization where you want to create a new user.

2. Confirm that an administrator user configured an LDAP server, and that the LDAP server was associated with the organization where you want to create a user account.

3. Click **Users > Users**.

   The **Users** page appears.

4. Click **Add**.

   The **Add User** page appears.

5. (Optional) Type a **First Name** and **Last Name** for the user.

6. In the **Type** drop-down list, select **LDAP**. If **LDAP** does not appear in the drop-down list, add an LDAP server as described in Add an LDAP Server.

7. Select the **LDAP Server** where you want to authenticate the user.

8. Select an LDAP user from the **LDAP Users Found** drop-down box.

   The page populates the **Username** option with your selection.

9. View the **Username**. Tenable does not recommend modifying the **Username** since it must match the username on the LDAP server.

10. Select a **Time Zone**.
11. (Optional) Select a **Scan Result Default Timeframe**.

12. (Optional) Enable **Cached Fetching**.

13. Select a **Role**. For more information, see [User Roles](#).

14. Select a **Group**. For more information, see [Organizations and Groups](#).

15. (Optional) If you want to customize the group-related permissions for the user, modify the **Group Permissions** as described in [Custom Group Permissions](#).

16. (Optional) If you want to share an asset list with the user, select an **Asset**. For more information, see [Assets](#).

17. (Optional) Type **Contact Information** for the user.

18. Click **Submit**.

   Tenable.sc Director saves your configuration.
Add a SAML-Authenticated User

**Required User Role:** Administrator or organizational user with appropriate permissions. For more information, see [User Roles](#)

For more information about user account configuration options, see [User Accounts](#). To automatically add SAML-authenticated users by importing users from your SAML identity provider, see [Configure SAML User Provisioning](#).

Before you begin:

- Configure SAML authentication, as described in [Configure SAML Authentication Manually via the User Interface](#).

To add a SAML-authenticated user account as an administrator user:

1. Log in to Tenable.sc via the user interface.
2. Click **System > Users**.
   The **Users** page appears.
3. Click **Add**.
   The **Add User** page appears.
4. (Optional) Type a **First Name** and **Last Name** for the user.
5. In the **Type** drop-down box, select **SAML**. If **SAML** does not appear in the drop-down box, configure SAML authentication as described in [Configure SAML Authentication Manually via the User Interface](#).
6. In the **Username** box, type the user's SAML username exactly as it appears in your identity provider SAML configuration for this user.
7. Select a **Time Zone**.
8. (Optional) Select a **Scan Result Default Timeframe**.
9. (Optional) Enable **Cached Fetching**.
10. (Optional) Type **Contact Information** for the user.
11. Click **Submit**.

   Tenable.sc Director saves your configuration.

To add a SAML-authenticated user account as an organizational user:

1. Log in to Tenable.sc via the user interface. You must log in with a user account belonging to the organization where you want to create a new user.

2. Click **Users > Users**.

   The **Users** page appears.

3. Click **Add**.

   The **Add User** page appears.

4. (Optional) Type a **First Name** and **Last Name** for the user.

5. In the **Type** drop-down list, select **SAML**. If **SAML** does not appear in the drop-down list, configure SAML authentication as described in [Configure SAML Authentication Manually via the User Interface](#).

6. In the **Username** box, type the user's SAML username exactly as it appears in your identity provider SAML configuration for this user.

7. Select a **Time Zone**.

8. (Optional) Select a **Scan Result Default Timeframe**.

9. (Optional) Enable **Cached Fetching**.

10. Select a **Role**. For more information, see [User Roles](#).

11. Select a **Group**. For more information, see [Organizations and Groups](#).

12. (Optional) To customize the user's object and user account management permissions, modify the **Group Permissions** as described in [Custom Group Permissions](#).

13. (Optional) To share an asset list with the user, select an **Asset**. For more information, see [Assets](#).

14. (Optional) Type **Contact Information** for the user.

15. Click **Submit**.

   Tenable.sc Director saves your configuration.
Manage User Accounts

**Required User Role:** Administrator or organizational user with appropriate permissions. For more information, see [User Roles](#).

For more information about user accounts, see [User Accounts](#).

To view or edit a user account:

1. Log in to Tenable.sc Director via the user interface.
2. Click **System > Users** (administrator users) or **Users > Users** (organizational users).

   The **Users** page appears.
3. To filter the users that appear on the page, apply a filter as described in [Apply a Filter](#).
4. To view details for a user, see [View User Details](#).
5. To edit a user:
   a. In the row for the user, click the ⚙ menu.
      
      The actions menu appears.
   b. Click **Edit**.
      
      The **Edit User** page appears.
   c. Modify the user details.
   d. Click **Submit**.
      
      Tenable.sc Director saves your configuration.
6. To delete a user, see [Delete a User](#).
View User Details

**Required User Role:** Administrator or organizational user with appropriate permissions. For more information, see [User Roles](#).

For more information about user accounts, see [User Accounts](#).

To view details for a user:

1. Log in to Tenable.sc Director via the user interface.
2. Click **System > Users** (administrator users) or **Users > Users** (organizational users).
   
   The **Users** page appears.
3. In the row for the user, click the menu.
4. Click **View**.
   
   The **View User** page appears.
5. View the following information for the user:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>View general information for the user.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Created</strong> — The date the user was created.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Last Modified</strong> — The date the user was last modified.</td>
</tr>
<tr>
<td></td>
<td>- <strong>ID</strong> — The user ID.</td>
</tr>
<tr>
<td>Membership</td>
<td>View role and organization information for the user. For more information, see <a href="#">User Accounts</a>.</td>
</tr>
<tr>
<td>Contact Information</td>
<td>View contact information for the user. For more information, see <a href="#">User Accounts</a>.</td>
</tr>
<tr>
<td>API Key</td>
<td>If the user has API keys, view the access key for the user. For more information, see <a href="#">Enable API Key Authentication</a>.</td>
</tr>
</tbody>
</table>
**Required User Role:** Administrator

View linked user accounts associated with the user:

- **Linked Users** — If the user is an Administrator, view the linked Security Manager users.

- **Primary User** — If the user is a Security Manager, view the linked Administrator user.

For more information, see [Linked User Accounts](#).
Delete a User

**Required User Role:** Administrator or organizational user with appropriate permissions. For more information, see [User Roles](#).

If you want to migrate a user's objects, you must use a Security Manager account in the user's organization to delete the user. Other roles cannot migrate user objects.

**Note:** You cannot delete the first user created in any of your organizations. For more information, contact Tenable Support.

**Note:** If you want to delete an administrator user with linked user accounts, you must delete the linked accounts associated with the administrator before deleting the administrator, as described in [Delete a Linked User Account](#). For more information about linked user accounts, see [Linked User Accounts](#).

To delete a user:

1. Log in to Tenable.sc via the user interface.
2. Click **System > Users** (administrator users) or **Users > Users** (organizational users).
   
   The **Users** page appears.
3. In the row for the user you want to delete, click the menu.
   
   The actions menu appears.
4. Click **Delete**.
   
   A confirmation window appears.
5. (Optional) If you want to migrate the user's objects, click the toggle to migrate the user's objects to another user. Tenable.sc supports migrating:
   
   - Active scans, agent scans, and scan results
   - Custom assets, credentials, audit files, and scan policies
   - Blackout windows
   - Queries
   - Tickets and alerts
- ARCs
- Dashboards
- Reports, report images, report attributes, and report results

If you do not migrate the user's objects, Tenable.sc deletes the user's objects.

**Note:** You cannot migrate objects when deleting an Administrator user because all Administrator-created objects are shared across Tenable.sc and remain accessible after user deletion.

6. Click **Delete**.

Tenable.sc deletes the user.
Linked User Accounts

If a user needs to perform administrator and non-administrator tasks in Tenable.sc Director, you can configure \textit{linked user accounts} to allow an Administrator user to switch to one or more Security Manager users without logging out and logging back in to Tenable.sc Director.

Users with linked user accounts can use a single set of login credentials to log in to Tenable.sc Director as an Administrator, then switch to a linked Security Manager, from one linked Security Manager to another, or from a linked Security Manager to the linked Administrator. You do not need to re-authenticate to switch between linked user accounts after logging in as the linked Administrator.

The following restrictions apply to linked user accounts:

- Each Administrator can have one linked Security Manager per organization.
- Linked Security Managers can be associated with only one Administrator user account.
- Linked Security Managers cannot log in to Tenable.sc Director directly. You must log into the Administrator account associated to the linked Security Manager, then switch users.
- You cannot convert a standalone user account to a linked user account.
- You cannot convert a linked user account to a standalone user account. To unlink a Security Manager user from an Administrator user, delete the linked Security Manager, then create a standalone Security Manager.

For more information about user accounts in Tenable.sc Director, see \textit{User Access} and \textit{User Roles}.

For more information about linked user accounts, see:

- \textbf{Add a Linked User}
- \textbf{Switch to a Linked User Account}
- \textbf{Delete a Linked User Account}
Add a Linked User

Required User Role: Administrator

To allow an Administrator user to switch to one or more Security Manager users without logging out and logging back in to Tenable.sc, add a linked user account to the Administrator. The following restrictions apply to linked user accounts:

- You cannot convert a standalone user account to a linked user account.
- Each Administrator can have one linked Security Manager per organization.
- Linked Security Managers can only be associated with a single Administrator user account.

For more information about linked user accounts, see Linked User Accounts. For more information about user account configuration options, see User Accounts.

To add a linked Security Manager to an Administrator:

1. Log in to Tenable.sc via the user interface.
2. Click System > Users.
   The Users page appears.
3. In the row for the Administrator for which you want to add a linked user, click the menu.
   The actions menu appears.
4. Click Add Linked User.
   The Add User page appears. Tenable.sc pre-populates the First Name, Last Name, and Contact Information fields with values from the administrator user account.
5. Select an Organization.
6. (Optional) Modify the First Name and Last Name for the user.
7. Type a Username for the user.
8. Select a Time Zone.
9. (Optional) Select a Scan Result Default Timeframe.
10. (Optional) Enable Cached Fetching.
11. (Optional) Modify the **Contact Information** for the user.

12. Click **Submit**.

   Tenable.sc Director saves your configuration.

What to do next:

- Switch between linked Administrator and Security Manager user accounts, as described in [Switch to a Linked User Account](#).
Switch to a Linked User Account

**Required User Role:** Administrator with linked user accounts or a Security Manager linked to an Administrator. For more information, see [User Roles](#).

Linked users can switch from the linked Administrator to a linked Security Manager, from one linked Security Manager to another, or from a linked Security Manager to the linked Administrator user. For more information about linked user accounts, see [Linked User Accounts](#).

Before you begin:
- Configure one or more linked user accounts, as described in [Add a Linked User](#).

To switch to a linked user account:

1. Log in to Tenable.sc Director via the user interface.
2. **Note:** You must log into the Administrator user associated to the linked Security Manager, then switch between linked users. Linked Security Managers cannot log in to Tenable.sc Director directly.
3. Click **Username > Switch User**.
   
   The **Switch To Linked Account** window appears.
4. Click the name of the linked user you want to switch to.
5. Click **Switch**.
   
   Tenable.sc Director logs you in as the selected user.
   
   The username menu updates to show the linked account name and associated organization.
Delete a Linked User Account

**Required User Role:** Administrator

If you want to remove a linked user account, you must delete the linked account. You cannot convert a linked user account into a standalone user account. For more information about linked user accounts, see [Linked User Accounts](#).

**Note:** If you want to delete an administrator user with linked user accounts, you must delete the administrator's linked accounts before deleting the administrator.

To delete a linked user account:

1. Log in to Tenable.sc Director via the user interface.
2. Click **System > Users**.
   
The **Users** page appears.
3. Apply a filter to view the organization for the user you want to delete, as described in [Apply a Filter](#).
4. In the row for the user you want to delete, click the **menu**.
   
The actions menu appears.
5. Click **Delete**.
   
A confirmation window appears.
6. (Optional) If you want to migrate the user's objects, click the toggle to migrate the user's objects to another user. Tenable.sc Director supports migrating:
   
   - Active scans, agent scans, and scan results
   - Custom assets, credentials, audit files, and scan policies
   - Blackout windows
   - Queries
   - Tickets and alerts
   - ARCs
- Dashboards
- Reports, report images, report attributes, and report results

If you do not migrate the user's objects, Tenable.sc Director deletes the user's objects.

**Note:** You cannot migrate objects when deleting an Administrator user because all Administrator-created objects are shared across Tenable.sc Director and remain accessible after user deletion.

7. Click **Delete**.

Tenable.sc Director deletes the user.
Custom Group Permissions

When creating or editing a user account, you can customize a user's group permissions.

- Your selection in the Group field assigns the user to a group.
- Your selections in the Group Permissions section grant the user resource (user and object) permissions in their assigned group and other groups.

For more information about organizations and groups, see Organizations and Groups.

In the Group Permissions section, the Manage All Users and Manage All Objects sliders enable or disable all of the settings in the User Permission and Object Permission columns, respectively. By default, the system enables all permissions for all groups. You can clear the check boxes in each group row to restrict the user's ability to perform the following actions on the resources within a group.

<table>
<thead>
<tr>
<th>Resources Controlled by Manage Users/User Permissions</th>
<th>Resources Controlled by Manage Objects/Object Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Users (edit and delete)</td>
<td>• Reports (launch, stop, copy, delete, and sometimes edit)</td>
</tr>
<tr>
<td>• Groups (edit and delete)</td>
<td>Note: A user can only edit reports within their assigned group, even if you grant them Object Permissions for another group.</td>
</tr>
<tr>
<td></td>
<td>• Report results (publish, email, copy, and delete)</td>
</tr>
<tr>
<td></td>
<td>• Report images (delete)</td>
</tr>
<tr>
<td></td>
<td>• Report attributes (delete)</td>
</tr>
<tr>
<td></td>
<td>• Scan results (stop, pause, and delete)</td>
</tr>
<tr>
<td></td>
<td>• Assets (edit, share, and delete)</td>
</tr>
</tbody>
</table>

Copyright © 2020 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.
### Resources Controlled by Manage Users/User Permissions

- Alerts (edit and delete)
- Audit files (edit, share, and delete)
- Tickets (edit, resolve, and close)
- Queries (edit, share, and delete)
- Dashboards (edit, share, copy, and delete)

### Resources Controlled by Manage Objects/Object Permissions

- Alerts (edit and delete)
- Audit files (edit, share, and delete)
- Tickets (edit, resolve, and close)
- Queries (edit, share, and delete)
- Dashboards (edit, share, copy, and delete)

### Examples

Consider the following examples for a user assigned to *Group1*.

#### Control Permissions to Resources in the User's Assigned Group

- If you select the **User Permissions** and/or **Object Permissions** check boxes in the *Group1* row, the user can perform actions for all resources in *Group1*, including the resources owned by other users.

- If you clear the **User Permissions** and/or **Object Permissions** check boxes in the *Group1* row, the user cannot perform actions on resources owned by other users in *Group1*.

#### Control Permissions to Resources in Other Groups

- If you select the **User Permissions** and/or **Object Permissions** check boxes in the *Group2* row, the user can perform actions for all resources in *Group2*, including the resources owned by other users.

Note: Although the user receives many permissions for resources in *Group2*, the user cannot edit reports owned by *Group2* users. Users must be assigned to *Group2* and have **Object Permissions** selected in order to edit reports, active scans, and agent scans.

- If you clear the **User Permissions** and/or **Object Permissions** check boxes in the *Group2* row, the user cannot perform actions on resources owned by other users in *Group2*.
Generate API Keys

**Required User Role:** Administrator or organizational user with appropriate permissions. For more information, see [User Roles](#).

API keys allow you to authenticate as a specific user for Tenable.sc API requests. Administrators can generate API keys for any user account. Other roles can generate API keys for user accounts with the same role. For more information, see [API Key Authentication](#).

**Note:** If you generate API keys for a user that already has API keys, the old keys will be replaced. If you delete existing keys or generate new API keys for a user, Tenable.sc deauthorizes API requests attempted with the old keys.

Before you begin:

- Enable API keys to allow users to perform API key authentication, as described in [Enable API Key Authentication](#).

To generate API keys:

1. Log in to Tenable.sc Director via the user interface.
2. Click **System > Users** (administrator users) or **Users > Users** (organizational users).
   The Users page appears.
3. In the row for the user for which you want to generate an API key, click the menu.
   The actions menu appears.
4. Click **Generate API Key**.
   A confirmation window appears.
5. Click **Generate**.
   The Your API Key window appears, displaying the access key and secret key for the user.
6. Save the API keys in a safe location.

**Note:** You cannot view API secret keys in the Tenable.sc interface after initial generation. If you lose your existing secret key, you must generate new API keys.
What to do next:

- Use the API keys to perform API requests, as described in [API Key Authorization](#) in the [Tenable.sc API Best Practices Guide](#).
Delete API Keys

**Required User Role:** Administrator or organizational user with appropriate permissions. For more information, see [User Roles](#).

After you delete a user's API keys, the deleted keys cannot be used for authentication in Tenable.sc API requests. To generate new API keys for a user, see [Generate API Keys](#). For more information, see [API Key Authentication](#).

To delete API keys:

1. Log in to Tenable.sc Director via the user interface.
2. Click **System** > **Users** (administrator users) or **Users** > **Users** (organizational users).
   - The **Users** page appears.
3. In the row for the user for which you want to delete API keys, click the ₪ menu.
   - The actions menu appears.
4. Click **Delete API Key**.
   - A confirmation window appears.
5. Click **Delete**.
   - The system deletes the API keys.
LDAP Authentication

Adding LDAP servers allows you to use one or more external LDAP servers for Tenable.sc Director user account authentication. LDAP authentication enhances the security of Tenable.sc Director by inheriting password complexity requirements from environments mandated by security policy.

After you configure an LDAP server, you must create Tenable.sc Director user accounts for each LDAP user you want to grant access. For more information, see Add an LDAP-Authenticated User.

You can also use configured LDAP servers as LDAP query assets. For more information, see Assets.

**Note:** Tenable.sc Director does not support Microsoft Active Directory Lightweight Directory Services (AD LDS) servers for LDAP authentication.

**Note:** Tenable.sc Director cannot retrieve more than one page of LDAP results. If Tenable.sc Director asset list or user authentication queries are not retrieving all expected results, consider modifying your LDAP pagination control settings to increase the results per page.

For more information, see Add an LDAP Server and Delete an LDAP Server.

Configure the LDAP settings as directed by your LDAP server administrator. Click Test LDAP Settings to validate the connection.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Settings</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>A unique name for the LDAP server.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) A description for the LDAP server.</td>
</tr>
<tr>
<td>Hostname</td>
<td>The IP address or DNS name of the LDAP server.</td>
</tr>
<tr>
<td>Port</td>
<td>The remote LDAP port. Confirm the selection with your LDAP server administrators.</td>
</tr>
<tr>
<td>Encryption</td>
<td>(Optional) If the LDAP server encrypts communications, the encryption method: Transport Layer Security (STARTTLS) or LDAP over SSL (LDAPS).</td>
</tr>
<tr>
<td>Username /</td>
<td>(Optional) If required by the server, the username and password for an account</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password</td>
<td>on the LDAP server with credentials to search for user data. For example, Active Directory servers require an authenticated search. Format the username as provided by the LDAP server.</td>
</tr>
<tr>
<td><strong>Tip:</strong> It is recommended to use passwords that meet stringent length and complexity requirements.</td>
<td></td>
</tr>
<tr>
<td>LDAP Schema Settings</td>
<td></td>
</tr>
<tr>
<td>Base DN</td>
<td>The LDAP search base used as the starting point to search for the user data.</td>
</tr>
<tr>
<td>User Object Filter</td>
<td>(Optional) The string you want to use to create a search based on a location or filter other than the default search base or attribute.</td>
</tr>
<tr>
<td>User Schema Settings</td>
<td>(Optional, if you plan to use the LDAP server only as an LDAP query asset.)</td>
</tr>
<tr>
<td>Username Attribute</td>
<td>The attribute name on the LDAP server that contains the username for the account. This is often specified by the string <code>sAMAccountName</code> in Active Directory servers that may be used by LDAP. Contact your LDAP server administrator for the correct value.</td>
</tr>
<tr>
<td>E-mail Attribute</td>
<td>The attribute name on the LDAP server that contains the email address for the account. This is often specified by the string <code>mail</code> in Active Directory servers that may be used by LDAP. Contact your LDAP server administrator for the correct value.</td>
</tr>
<tr>
<td>Phone Attribute</td>
<td>The attribute name on the LDAP server that contains the telephone number for the account. This is often specified by the string <code>telephoneNumber</code> in Active Directory servers that may be used by LDAP. Contact your LDAP server administrator for the correct value.</td>
</tr>
<tr>
<td>Name Attribute</td>
<td>The attribute name on the LDAP server that contains the name associated with the account. This is often specified by the string <code>CN</code> in Active Directory servers that may be used by LDAP. Contact your LDAP administrator for the correct value.</td>
</tr>
<tr>
<td>Access Settings</td>
<td></td>
</tr>
<tr>
<td>Organizations</td>
<td>The Tenable.sc Director organizations you want to authenticate using this LDAP server.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Advanced Settings</td>
<td></td>
</tr>
<tr>
<td>Lowercase</td>
<td>When enabled, Tenable.sc Director modifies the usernames sent by the LDAP server to use only lowercase characters. Tenable recommends keeping this option disabled.</td>
</tr>
<tr>
<td>DNS Field</td>
<td>The LDAP server parameter used in LDAP server requests to filter the returned asset data. Tenable recommends using the default value provided by Tenable.sc Director.</td>
</tr>
<tr>
<td>Time Limit</td>
<td>The number of seconds you want Tenable.sc Director to wait for search results from the LDAP server. Tenable recommends using the default value provided by Tenable.sc Director.</td>
</tr>
</tbody>
</table>

**Note:** Access to Active Directory is performed via AD's LDAP mode. When using multiple AD domains, LDAP access may be configured to go through the Global Catalog. Port 3268 is the default non-SSL/TLS setting, while port 3269 is used for SSL/TLS connections by default. More general information about LDAP searches via the Global Catalog may be found at: [http://technet.microsoft.com/en-us/library/cc728188(v=ws.10).aspx](http://technet.microsoft.com/en-us/library/cc728188(v=ws.10).aspx).
Add an LDAP Server

**Required User Role:** Administrator

For more information about LDAP server options, see [LDAP Authentication](#).

To add an LDAP server connection:

1. Log in to Tenable.sc via the user interface.
2. Click **Resources > LDAP Servers**.
3. Click **Add**.
4. Configure the following settings as described in the [Options](#) table:
   - Server Settings
   - LDAP Schema Settings
   - User Schema Settings
   - Access Settings
5. If necessary, modify the default [Advanced Settings](#).
6. Click **Test LDAP Settings** to validate the LDAP server connection.
7. Click **Submit**.

What to do next:

- Add user accounts for each LDAP user you want to grant access to Tenable.sc, as described in [Add an LDAP-Authenticated User](#).
Delete an LDAP Server

**Required User Role:** Administrator

For more information, see [LDAP Authentication](#).

To delete an LDAP server connection:

**Note:** If you delete a connection to an LDAP server, the users associated with that server cannot log in to Tenable.sc Director. Tenable recommends reconfiguring associated user accounts before deleting LDAP server connections.

1. Log in to Tenable.sc Director via the user interface.

2. Click **Resources > LDAP Servers**.

3. In the row for the server connection you want to delete, click the ⚙ menu.
   
The actions menu appears.

4. Click **Delete**.
   
   A confirmation window appears.

5. Click **Delete**.

   Tenable.sc Director deletes the LDAP server.
LDAP Servers with Multiple OUs

Tenable’s Tenable.sc Director LDAP configuration does not support the direct addition of multiple Organizational Units (OUs) in the LDAP configuration page. Two deployment options are possible for those with multiple OUs.

For general information about LDAP Servers, see LDAP Authentication.

Option 1 (Recommended)

When you complete these changes, new users who are members of this group can log in immediately. No restart is required.

Before you begin:

- In LDAP, add a new group for Tenable.sc Director users.
- In LDAP, allow existing Active Directory users to become members of the new group.

To configure LDAP with multiple OUs (Option 1):

1. Log in to Tenable.sc Director via the user interface.
2. Click Resources > LDAP Servers.
3. Add the LDAP server, as described in Add an LDAP Server.

   Note: Use the Distinguished Name (DN) of the new group as the Search Base (e.g., CN=Tenable.sc,DC=target,DC=example,DC=com).

4. Log out of Tenable.sc Director.
5. Log in to Tenable.sc Director as the organizational user you want to manage the users.
6. Create a user account for each Active Directory user in the new group, as described in Add an LDAP-Authenticated User.
Set the LDAP **Search String** as `=*`. 

![Image of LDAP configuration screen](image)

**Option 2**

Use a high level **Search Base** in the LDAP configuration. For example: `DC=target,DC=example,DC=com`.

The example above could be used along with a **Search String** for global usage. As another example, you might use this search string, when used in the configuration, applies to all LDAP searches:

`memberOf=CN=nested1,OU=cftest1,DC=target,DC=example,DC=com`

**Note:** This option is limited to 128 characters.

To configure LDAP with multiple OUs (Option 2):

1. Log in to Tenable.sc Director via the user interface.
2. Click **Resources > LDAP Servers.**
3. Begin configuring the LDAP server, as described in [Add an LDAP Server](#).
4. Click **Test LDAP Settings** to test configurations.

5. Log out of Tenable.sc Director.

6. Log in to Tenable.sc Director as the organizational user you want to manage the users.

7. Create a user account for each Active Directory user, as described in Add an LDAP-Authenticated User.
SAML Authentication

You can configure SAML authentication so that Tenable.sc Director users can use identity provider-initiated single sign-on (SSO) when logging in to Tenable.sc Director. Tenable.sc Director supports:

- SAML 2.0-based authentication (e.g., Okta, OneLogin, Microsoft ADFS, etc.)
- Shibboleth 1.3 authentication

For more information, see:

- Configure SAML Authentication Automatically via the User Interface
- Configure SAML Authentication Manually via the User Interface
- Configure SAML Authentication via the SimpleSAML Module

After you configure SAML authentication, create Tenable.sc Director user accounts for each SAML user you want to grant access.

- To manually add SAML-authenticated users in Tenable.sc Director, see Add a SAML-Authenticated User.
- To automatically add SAML-authenticated users by importing users from your SAML identity provider, see User Provisioning.

Then, users with SAML-authenticated accounts can log in to Tenable.sc Director using the Sign In Using Identity Provider button, as described in Log In to the Web Interface.

Considerations for Advanced SAML Features

Because Tenable.sc Director cannot accept private keys to decrypt SAML assertions, Tenable.sc Director does not support SAML assertion encryption. If you want to configure SAML authentication in Tenable.sc Director, choose an identity provider that does not require assertion encryption and confirm that assertion encryption is not enabled.

For information about Tenable.sc Director communications encryption, see Encryption Strength.

Note: Tenable Support does not assist with configuring or troubleshooting advanced SAML features.

User Provisioning
You can configure user provisioning to allow Tenable.sc Director to automatically create and update Tenable.sc Director user accounts by importing user data from your SAML identity provider. When user provisioning is enabled and a user who does not have a Tenable.sc Director user account logs in using your SAML identity provider, Tenable.sc Director automatically creates a user account for them in Tenable.sc Director.

Tenable.sc Director creates users using data from attribute fields you map to the corresponding fields in your SAML identity provider. If you enable **User Data Sync**, each time a user logs into Tenable.sc Director using your SAML identity provider, Tenable.sc Director updates any mapped attribute fields in Tenable.sc Director with values from the corresponding fields in your SAML identity provider.

For more information, see [Configure SAML User Provisioning](#).

### SAML Authentication Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML</td>
<td>Specifies whether SAML authentication is enabled or disabled. If you disable SAML, the system clears your SAML configuration settings and prevents SAML-authenticated user accounts from accessing Tenable.sc.</td>
</tr>
<tr>
<td>Source</td>
<td>Specifies your SAML configuration method:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Import</strong> — Configure SAML authentication by uploading the metadata file provided by your identity provider, as described in <a href="#">Configure SAML Authentication Automatically via the User Interface</a>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Entry</strong> — Configure SAML authentication by manually configuring SAML options using data from the metadata file provided by your identity provider, as described in <a href="#">Configure SAML Authentication Manually via the User Interface</a>.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the identity provider you are using: <strong>SAML 2.0</strong> (e.g., Okta, OneLogin, etc.) or <strong>Shibboleth 1.3</strong>.</td>
</tr>
<tr>
<td>Entity ID</td>
<td>The name of the Entity ID attribute. Type the attribute exactly as it appears in your identity provider SAML configuration.</td>
</tr>
<tr>
<td>Identity Provider</td>
<td>The identity provider identifier string.</td>
</tr>
</tbody>
</table>

**Tip:** This is the **Federation Service Identifier** value in Microsoft ADFS.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Provider (IdP)</td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>• The <strong>Identity Provider Issuer</strong> value in Okta.</td>
</tr>
<tr>
<td></td>
<td>• The <strong>Federation Service Identifier</strong> value in Microsoft ADFS.</td>
</tr>
<tr>
<td>Username Attribute</td>
<td>The name of the SAML username attribute. Type the attribute exactly as it appears in your identity provider SAML configuration.</td>
</tr>
<tr>
<td></td>
<td>For example, if your SAML username attribute is <strong>NameID</strong>, specify <strong>NameID</strong> to instruct Tenable.sc to recognize users who match the format NameID=username.</td>
</tr>
<tr>
<td>Single Sign-on Service</td>
<td>The identity provider URL where users log in via single sign-on. Type the URL exactly as it appears in your identity provider SAML metadata.</td>
</tr>
<tr>
<td>Single Logout Service</td>
<td>The identity provider URL where users log out. Type the URL exactly as it appears in your identity provider SAML metadata.</td>
</tr>
<tr>
<td>Certificate Data</td>
<td>The text of the identity provider's X.509 SSL certificate, without the ===BEGIN CERT=== and the ===END CERT=== strings.</td>
</tr>
<tr>
<td>User Provisioning</td>
<td>When enabled, allows Tenable.sc to create Tenable.sc user accounts by importing user data from your SAML identity provider. For more information, see <a href="#">Configure SAML User Provisioning</a>.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> If you want to delete a Tenable.sc user that was created via SAML user provisioning, delete the user from your SAML identity provider. If you delete a user in Tenable.sc that was created via SAML user provisioning without deleting the user in your SAML identity provider, Tenable.sc will automatically re-create the user in Tenable.sc the next time they log in using your SAML identity provider.</td>
</tr>
<tr>
<td>User Data Sync</td>
<td>(If <strong>User Provisioning</strong> is enabled) When enabled, Tenable.sc automatically updates contact information for Tenable.sc users created via SAML user provisioning. For more information, see <a href="#">Configure SAML User Provisioning</a>.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> If you want to edit a Tenable.sc user that was created via SAML user provisioning and <strong>User Data Sync</strong> is enabled, edit the user in your SAML identity provider. Otherwise, your changes will be overwritten the next time the user logs in to Tenable.sc using your SAML identity provider.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Tip: Tenable.sc does not update required fields (Organization ID, Group ID, and Role ID). To change the organization, group, or role for a user created via SAML user provisioning, see Manage User Accounts.</td>
<td></td>
</tr>
</tbody>
</table>
Configure SAML Authentication Automatically via the User Interface

**Required User Role:** Administrator

You can use this method to configure most types of SAML authentication via the Tenable.sc Director user interface. If you encounter issues with this method (e.g., when configuring Microsoft ADFS), try the module method described in [Configure SAML Authentication via the SimpleSAML Module](#).

For more information about SAML authentication and SAML authentication options, see [SAML Authentication](#).

Before you begin:

- Save your identity provider SAML metadata file to a directory on your local computer.

To automatically configure SAML authentication for Tenable.sc Director users:

1. Log in to Tenable.sc Director via the user interface.
2. In the top navigation bar, click **System > Configuration**.
   
   The **Configuration** page appears.
3. Click the **SAML** button.
   
   The **SAML Configuration** page appears.
4. In the **General** section, confirm the **SAML** toggle is enabled.
   
   If you want to disable SAML authentication for Tenable.sc Director users, click the toggle.
5. In the **Source** drop-down box, select **Import**.
   
   The page updates to display additional options.
6. In the **Type** drop-down box, select **SAML 2.0** (e.g., Okta, OneLogin, etc.) or **Shibboleth 1.3**.
7. Click **Choose File** and browse to the SAML metadata file from your identity provider.

**Note:** The metadata file must match the **Type** you selected. If Tenable.sc Director rejects the file, contact your identity provider for assistance.
8. Click **Submit**.

Tenable.sc Director saves your configuration.

What to do next:

- Click **Download SAML Configuration XML**, save the `.xml` file locally, and use it to configure your identity provider SAML configuration. For more information, see [SAML Authentication XML Configuration Examples](#).

- Add SAML-authenticated user accounts.
  
  - To manually add SAML-authenticated users in Tenable.sc Director, see [Add a SAML-Authenticated User](#).
  
  - To automatically add SAML-authenticated users by importing users from your SAML identity provider, see [Configure SAML User Provisioning](#).

- Instruct users to log in to Tenable.sc Director using the **Sign In Using Identity Provider** button, as described in [Log In to the Web Interface](#).
Configure SAML Authentication Manually via the User Interface

**Required User Role:** Administrator

You can use this method to configure most types of SAML authentication via the Tenable.sc Director interface. However, you may prefer a more streamlined method:

- To configure SAML Authentication automatically, use the method described in [Configure SAML Authentication Automatically via the User Interface](#).
- If you encounter issues with either method (e.g., when configuring Microsoft ADFS), try the module method described in [Configure SAML Authentication via the SimpleSAML Module](#).

For more information about SAML authentication and SAML authentication options, see [SAML Authentication](#).

**Before you begin:**

- Save your identity provider SAML metadata file to a directory on your local computer.

To configure SAML authentication for Tenable.sc Director users:

1. Log in to Tenable.sc Director via the user interface.
2. In the top navigation bar, click **System > Configuration**.
   
   The **Configuration** page appears.
3. Click the **SAML** button.
   
   The **SAML Configuration** page appears.
4. In the **General** section, confirm the **SAML** toggle is enabled.
   
   If you want to disable SAML authentication for Tenable.sc Director users, click the toggle.
5. In the **Source** drop-down box, select **Entry**.
   
   The page updates to display additional options.
6. In the **SAML Settings** section, configure the options:
   
a. In the **Type** drop-down box, select **SAML 2.0** (e.g., Okta, OneLogin, etc.) or **Shibboleth 1.3**.
   
b. In the **Entity ID** box, type the name of the Entity ID attribute exactly as it appears in your identity provider SAML configuration.
   
c. In the **Identity Provider (IdP)** box, type identity provider identifier string.
   
d. In the **Username Attribute** box, type the SAML username attribute exactly as it appears in your identity provider SAML configuration.
   
e. In the **Single Sign-on Service** box, type the identity provider URL where users log in via single sign-on exactly as it appears in your identity provider SAML metadata.
   
f. In the **Single Logout Service** box, type the identity provider URL where users log out exactly as it appears in your identity provider SAML metadata.
   
g. In the **Certificate Data** box, paste the text of the identity provider's X.509 SSL certificate, without the `===BEGIN CERT===` and the `===END CERT===` strings.
   
7. Click **Submit**.

   Tenable.sc Director saves your configuration.

What to do next:

- Click **Download SAML Configuration XML**, save the `.xml` file locally, and use it to configure your identity provider SAML configuration. For more information, see [SAML Authentication XML Configuration Examples](#).

- Add SAML-authenticated user accounts.
  
  - To manually add SAML-authenticated users in Tenable.sc Director, see [Add a SAML-Authenticated User](#).
  
  - To automatically add SAML-authenticated users by importing users from your SAML identity provider, see [Configure SAML User Provisioning](#).

- Instruct users to log in to Tenable.sc Director using the **Sign In Using Identity Provider** button, as described in [Log In to the Web Interface](#).
Configure SAML Authentication via the SimpleSAML Module

**Required User Role:** Administrator

If you encounter issues configuring SAML via the Tenable.sc interface, you can use a hidden SimpleSAML module to automatically configure SAML authentication.

For general information, see [SAML Authentication](#).

**Before you begin:**

- Save your identity provider SAML metadata file to a directory on your local computer.

**To configure SAML authentication via the SimpleSAML module:**

1. Log in to Tenable.sc Director via the user interface.
2. In the top navigation bar, click **System > Configuration**.
   
   The **Configuration** page appears.
3. Click the **SAML** button.
   
   The **SAML Configuration** page appears.
4. Type placeholder values into all SAML configuration options. You do not need to configure valid values.
5. Click **Submit**.
   
   Tenable.sc Director saves your configuration.
6. Log in to Tenable.sc Director via the CLI.
8. Copy and paste the following text into the file, between the `);` line and the `);` line:

```php
// This is a authentication source which handles admin authentication.
'admin' => array(
  // The default is to use core:AdminPassword, but it can be replaced with
  // any authentication source.
```
9. Save the file.

10. In a browser, navigate to https://<Tenable.sc IP address or hostname>/sam-
l/module.php/core/frontpage_config.php.

   The **SimpleSAML.php installation** page appears.

11. On the **Configuration** tab, click **Login as administrator**.

   The **Enter your username and password** page appears.

12. In the **Username** box, type **admin**.

13. In the **Password** box, type **admin**.

14. Click **Login**.

15. On the **Federation** tab, in the **Tools** section, click **XML to SimpleSAML.php metadata converter**.

   The **Metadata parser** page appears.

16. Click **Choose File** and select your identity provider SAML metadata file.

17. Click **Parse**.

   Tenable.sc Director validates the identity provider SAML metadata file. If the metadata file is sup-
   ported, Tenable.sc Director populates the XML metadata box with content from your metadata
   file. If the metadata file is not supported, you cannot use it for SAML authentication in Tenable.sc
   Director.

18. In the **saml20-idp-remote** section, copy the text in the box.

19. Log in to Tenable.sc Director via the CLI.

20. Navigate to and open the /opt/sc/src/lib/SimpleSAML/metadata/saml20-idp-
 remote.php file (for SAML 2.0) or /opt/sc/src/lib/SimpleSAML/metadata/shib13-idp-
 remote.php file (for Shibboleth 1.3).

21. Paste the text into the file, after the <?php line.
22. Save the file.

23. Navigate to and open the /opt/sc/src/lib/SimpleSAML/config/authsources.php file again.

24. Confirm the idp URL in the authsources.php file matches the $metadata URL in the saml20-idp-remote.php or shib13-idp-remote.php file:

Valid authsources.php syntax example:

```php
'idp' => 'http://www.okta.com/abcdefghijKLmnopQr0s1'
```

Valid saml20-idp-remote.php or shib13-idp-remote.php syntax example:

```php
$metadata['http://www.okta.com/abcdefghijKLmnopQr0s1']
```

25. In a browser, navigate to https://<Tenable.sc IP address or hostname>/sam-

   l/module.php/core/frontpage_config.php.

   The SimpleSAML.php installation page appears.

26. On the Authentication tab, click Test configured authentication sources.

   The Test authentication sources page appears.

27. Click 1.

   Your identity provider login page appears.

28. Log in to your identity provider.

   The SAML 2.0 SP Demo Example page appears. If this page does not appear, the configuration
did not succeed.

What to do next:

- In the Tenable.sc interface, on the SAML Configuration page, click Download
SAML Configuration XML, save the .xml file locally, and use it to configure your identity pro-
vider SAML configuration. For more information, see SAML Authentication XML Configuration
Examples.
• Add SAML-authenticated user accounts.
  • To manually add SAML-authenticated users in Tenable.sc Director, see Add a SAML-Authenticated User.
  • To automatically add SAML-authenticated users by importing users from your SAML identity provider, see Configure SAML User Provisioning.
• Instruct users to log in to Tenable.sc Director using the Sign In Using Identity Provider button, as described in Log In to the Web Interface.
Configure SAML User Provisioning

**Required User Role:** Administrator

You can enable user provisioning to automatically create SAML-authenticated users in Tenable.sc Director by importing user accounts from your SAML identity provider. When user provisioning is enabled, users who log into your SAML identity provider are automatically created in Tenable.sc Director. To manually create SAML-authenticated users in Tenable.sc Director, see [Add a SAML-Authenticated User](#).

For more information about user account configuration options, see [User Accounts](#).

**Before you begin:**

- Configure SAML authentication, as described in [Configure SAML Authentication Manually via the User Interface](#).

**To import SAML-authenticated user accounts from your SAML identity provider:**

1. Log in to Tenable.sc Director via the user interface.

2. In the top navigation bar, click **System > Configuration**.

   The **Configuration** page appears.

3. Click the **SAML** button.

   The **SAML Configuration** page appears.

4. In the **SAML Settings** section, click the toggle to enable **User Provisioning**.

5. (Optional) To automatically update contact information for imported SAML-authenticated users, click the **User Data Sync** toggle.

   **Tip:** When **User Data Sync** is enabled, Tenable.sc Director automatically updates all mapped user attributes in Tenable.sc Director with values from your SAML identity provider. If you want to edit a Tenable.sc Director user that was created via SAML user provisioning, edit the user in your SAML identity provider. Otherwise, your changes will be overwritten the next time the user logs in to Tenable.sc Director using your SAML identity provider.

6. Click **Submit**.

   Tenable.sc Director saves your configuration.
What to do next:

- In your SAML identity provider, map the required Tenable.sc user attribute fields to the corresponding fields for users in your identity provider: **Organization ID, Group ID, and Role ID**.

**Note:** Tenable.sc Director uses the fields listed in the **Attribute Mapping** section to create and update users in Tenable.sc Director. Any Tenable fields that you map to corresponding fields in your SAML identity provider are populated when Tenable.sc Director imports SAML users into Tenable.sc Director. If you enable **User Data Sync**, each time a user logs into Tenable.sc Director using your SAML identity provider, Tenable.sc Director updates any mapped attribute fields in Tenable.sc Director with values from the corresponding fields in your SAML identity provider.
SAML Authentication XML Configuration Examples

Identity provider SAML configurations vary widely, but you can use the following examples to guide your SAML-side configurations.

- **OneLogin Example**
- **Okta Example**
- **Microsoft ADFS Example**

### OneLogin Example

In the OneLogin SAML configuration, paste data from your .xml download file.

<table>
<thead>
<tr>
<th>OneLogin Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relay State</td>
<td>Leave this field blank.</td>
</tr>
<tr>
<td>Audience</td>
<td>Type tenable.sc.</td>
</tr>
<tr>
<td>Recipient</td>
<td>Type https://&lt;Tenable.sc host&gt;/saml/module.php/saml/sp/saml2-acs.php/1, where &lt;Tenable.sc host&gt; is the IP address or hostname for Tenable.sc Director.</td>
</tr>
<tr>
<td>ACS (Consumer) URL</td>
<td>Type -*.</td>
</tr>
<tr>
<td>ACS (Consumer) URL</td>
<td>Type https://&lt;Tenable.sc host&gt;/saml/module.php/saml/sp/saml2-acs.php/1, where &lt;Tenable.sc host&gt; is the IP address or hostname for Tenable.sc Director.</td>
</tr>
<tr>
<td>Single Logout URL</td>
<td>Type https://&lt;Tenable.sc host&gt;/saml/module.php/saml/index.php?sls, where &lt;Tenable.sc host&gt; is the IP address or hostname for Tenable.sc Director.</td>
</tr>
</tbody>
</table>

### Okta Example

In the Okta SAML configuration, paste data from your .xml download file.
<table>
<thead>
<tr>
<th><strong>Okta Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Single Sign On URL</td>
<td>Type <code>https://&lt;Tenable.sc host&gt;/saml/module.php/saml/sp/saml2-acsp.php/1</code>, where <code>&lt;Tenable.sc host&gt;</code> is the IP address or hostname for Tenable.sc Director.</td>
</tr>
<tr>
<td>Recipient URL</td>
<td>Type <code>https://&lt;Tenable.sc host&gt;/saml/module.php/saml/sp/saml2-acsp.php/1</code>, where <code>&lt;Tenable.sc host&gt;</code> is the IP address or hostname for Tenable.sc Director.</td>
</tr>
<tr>
<td>Destination URL</td>
<td>Type <code>https://&lt;Tenable.sc host&gt;/saml/module.php/saml/sp/saml2-acsp.hp/1</code>, where <code>&lt;Tenable.sc host&gt;</code> is the IP address or hostname for Tenable.sc Director.</td>
</tr>
<tr>
<td>Audience Restriction</td>
<td>Type <code>tenable.sc</code>.</td>
</tr>
<tr>
<td>Default Relay State</td>
<td>Leave this field blank.</td>
</tr>
<tr>
<td>Name ID Format</td>
<td>Set to Unspecified.</td>
</tr>
<tr>
<td>Response</td>
<td>Set to Signed.</td>
</tr>
<tr>
<td>Assertion Signature</td>
<td>Set to Signed.</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>Set to RSA_SHA256.</td>
</tr>
<tr>
<td>Digest Algorithm</td>
<td>Set to SHA256.</td>
</tr>
<tr>
<td>Assertion Encryption</td>
<td>Set to Unencrypted.</td>
</tr>
<tr>
<td>SAML Single Logout</td>
<td>Set to Disabled.</td>
</tr>
<tr>
<td>authnContextClassRef</td>
<td>Set to PasswordProtectedTransport.</td>
</tr>
<tr>
<td>Honor Force Authentication</td>
<td>Set to Yes.</td>
</tr>
<tr>
<td>SAML Issuer ID</td>
<td>Type <code>http://www.okta.com/${org.externalKey}</code>.</td>
</tr>
<tr>
<td>Attribute Statements</td>
<td></td>
</tr>
<tr>
<td>Okta Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>FirstName</td>
<td>Set to <strong>Name Format</strong>: Unspecified and <strong>Value</strong>: user.firstName.</td>
</tr>
<tr>
<td>LastName</td>
<td>Set to <strong>Name Format</strong>: Unspecified and <strong>Value</strong>: user.lastName.</td>
</tr>
<tr>
<td>Email</td>
<td>Set to <strong>Name Format</strong>: Unspecified and <strong>Value</strong>: user.email.</td>
</tr>
<tr>
<td>username</td>
<td>Set to <strong>Name Format</strong>: Unspecified and one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Value</strong>: user.displayName, if your Tenable.sc Director user account usernames are full names (e.g., Jill Smith).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Value</strong>: user.email, if your Tenable.sc Director user account usernames are email addresses (e.g., <a href="mailto:jsmith@website.com">jsmith@website.com</a>).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Value</strong>: user.login, if your Tenable.sc Director user account usernames are name-based text strings (e.g., jsmith).</td>
</tr>
</tbody>
</table>

**Microsoft ADFS Example**

In the Microsoft ADFS configuration, paste data from your .xml download file.

<table>
<thead>
<tr>
<th>Microsoft ADFS Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Authentication Methods window</td>
<td></td>
</tr>
<tr>
<td>Extranet</td>
<td>Select, at minimum, the <strong>Forms Authentication</strong> check box.</td>
</tr>
<tr>
<td>Intranet</td>
<td>Select, at minimum, the <strong>Forms Authentication</strong> check box.</td>
</tr>
<tr>
<td>Add Relying Party Trust wizard</td>
<td></td>
</tr>
<tr>
<td>Welcome section</td>
<td>• Select <strong>Claims aware</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Import data about the relying party from a file</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Browse to and select the SAML configuration .xml file you downloaded from Tenable.sc Director.</td>
</tr>
</tbody>
</table>

**Note:** If you see a warning that some content was skipped, click **Ok** to continue.
<table>
<thead>
<tr>
<th><strong>Microsoft ADFS Configuration</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify Display Name section</td>
<td>In the <strong>Display Name</strong> box, type your Tenable.sc Director FQDN.</td>
</tr>
<tr>
<td>Configure Certificate section</td>
<td>Browse to and select the encryption certificate you want to use.</td>
</tr>
<tr>
<td>Choose Access Control Policy section</td>
<td>Select the <strong>Permit everyone</strong> policy.</td>
</tr>
</tbody>
</table>
| Ready to Add Trust section      | - On the **Advanced** tab, select **SHA256** or the value dictated by your security policy.  
- On the **Identifiers** tab, confirm the information is accurate.  
- On the **Endpoints** tab, confirm the information is accurate. |
| Finish section                  | Select the **Configure claims issuance policy for this application** check box. |
| Edit Claim Issuance Policy window | Add one or more claim rules to specify the ADFS value you want Tenable.sc Director to use when authenticating SAML users. For example:  

**To transform an incoming claim:**  
1. In **Incoming claim type**, select **Email address** or **UPN**.  
2. In **Outgoing claim type**, select **Name ID**.  
3. In **Outgoing name ID format**, select **Transient Identifier**.  
4. Select the **Pass through all claim values** check box.  

**To send LDAP attributes as claim:**  
1. In **Attribute store**, select **Active Directory**.  
2. In **LDAP Attribute**, select **E-Mail Addresses**.  
3. In **Outgoing Claim Type**, select **E-Mail Addresses**.  

**Note:** Tenable Support does not assist with claim rules.
Certificate Authentication

You can use configure SSL client certificate authentication for Tenable.sc Director user account authentication. Tenable.sc Director supports:

- SSL client certificates
- smart cards
- personal identity verification (PIV) cards
- Common Access Cards (CAC)

Configuring certificate authentication is a multi-step process.

To fully configure SSL client certificate authentication for Tenable.sc Director user accounts:

1. Configure Tenable.sc Director to allow SSL client certificate authentication, as described in Configure Tenable.sc Director to Allow SSL Client Certificate Authentication.
2. Configure Tenable.sc Director to trust certificates from your CA, as described in Trust a Custom CA.
3. Add TNS-authenticated user accounts for the users you want to authenticate via certificate, as described in Add a TNS-Authenticated User.
4. (Optional) If you want to validate client certificates against a certificate revocation list (CRL), configure CRLs or OCSP in Tenable.sc Director, as described in Configure a CRL in Tenable.sc Director or Configure OCSP Validation in Tenable.sc Director.

What to do next:

- Instruct users to log in to Tenable.sc Director via certificate, as described in Log in to the Web Interface via SSL Client Certificate.
Configure Tenable.sc Director to Allow SSL Client Certificate Authentication

You must configure the Tenable.sc Director server to allow SSL client certificate connections. For complete information about certificate authentication, see Certificate Authentication.

To allow SSL client certificate authentication:

1. Open the /opt/sc/support/conf/sslverify.conf file in a text editor.
2. Edit the SSLVerifyClient setting:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none (default)</td>
<td>Tenable.sc Director does not accept SSL certificates for user authentication.</td>
</tr>
<tr>
<td>require</td>
<td>Tenable.sc Director requires a valid SSL certificate for user authentication.</td>
</tr>
<tr>
<td>optional</td>
<td>Tenable.sc Director accepts but does not require a valid SSL certificates for user authentication. If a user does not present a certificate, they can log in via username and password.</td>
</tr>
<tr>
<td>optional_no_ca</td>
<td>Tenable.sc Director accepts valid and invalid SSL certificates for user authentication.</td>
</tr>
</tbody>
</table>

**Note:** Depending on how they are configured, some web browsers may not connect to Tenable.sc when the optional setting is used.

**Tip:** This setting does not configure reliable user authentication, but you can use it to troubleshoot issues with your SSL connection and determine if the issue is key-based or CA-based.

3. Edit the SSLVerifyDepth setting to specify the length of the certificate chain you want Tenable.sc Director to accept for user authentication. For example:
• When set to 0, Tenable.sc Director accepts self-signed certificates.

• When set to 1, Tenable.sc Director does not accept intermediate certificates. Tenable.sc Director accepts self-signed certificates or certificates signed by known CAs.

• When set to 2, Tenable.sc Director accepts up to 1 intermediate certificate. Tenable.sc Director accepts self-signed certificates, certificates signed by known CAs, or certificates signed by unknown CAs whose certificate was signed by a known CA.

4. Save the file.

Tenable.sc Director saves your configuration.
Configure a CRL in Tenable.sc Director

**Required User Role:** Root user

You can enable a certificate revocation list (CRL) in Tenable.sc Director to prevent users from authenticating to Tenable.sc Director if their certificate matches a revocation in the CRL.

**Note:** Tenable Support does not assist with CRL creation or configuration in Tenable.sc Director.

Before you begin:

- Confirm that you have the mod_ssl Apache module installed on Tenable.sc Director.
- Back up the /opt/sc/data/CA/ directory in case you encounter issues and need to restore the current version.

To configure a CRL in Tenable.sc Director:

1. In a text editor, open the /opt/sc/support/conf/sslverify.conf file.
   a. Set the `SSLVerifyClient` setting to `Require` or `Optional`, as described in [SSLVerifyClient](#).
   b. Set the `SSLVerifyDepth` setting, as described in [SSLVerifyDepth](#).
   c. Save the file.
      
      Tenable.sc Director saves your configuration.

2. Restart Tenable.sc Director, as described in [Start, Stop, or Restart Tenable.sc Director](#).
   
   Tenable.sc Director restarts.

3. Confirm that your CA root configuration file contains the following parameters:
   - `crl_dir`
   - `database`
   - `crl`
   - `crl_extensions`
   - `default_crl_days`
For example:

```bash
... 
# Directory and file locations.
dir = /opt/sc/data/CA
crl_dir = /opt/sc/support/conf/crl
database = /opt/sc/support/conf/index.txt
# The root key and root certificate.
private_key = /opt/sc/support/conf/TenableCA.key
certificate = /opt/sc/data/CA/TenableCA.crt
# For certificate revocation lists.
crl = /opt/sc/support/conf/crl/ca.crl
crl_extensions = crl_ext
default_crl_days = 30
...
```

4. Save your CA root configuration file as `YourCAname.conf` in a subdirectory of `/opt/sc/support/conf/`.

5. Confirm the directories and files referenced in your `YourCAname.conf` file are present on Tenable.sc Director in a subdirectory of `/opt/sc/support/conf/`.

6. Configure Tenable.sc Director to trust your CA, as described in [Trust a Custom CA](#).

   Tenable.sc Director processes your CA.

7. Run the following command to enable the CRL in Tenable.sc Director:

   ```bash
   $ openssl ca -config <CA root configuration file directory> -gencrl -out <crl parameter value in the YourCAname.conf file>
   ```

   For example:

   ```bash
   $ openssl ca -config /opt/sc/support/conf/ca-root.conf -gencrl -out /opt/sc/support/conf/crl/ca.crl
   ```

   Tenable.sc Director creates the CRL file.
8. In a text editor, open the `/opt/sc/support/conf/vhostssl.conf` file.

   a. Add the following content at the end of the file:

   ```
   SSLCARevocationCheck <value>
   SSLCARevocationFile "<filepath>"
   ```

   Where `<value>` and `<filepath>` are:

<table>
<thead>
<tr>
<th>Content</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSLCARevocationCheck <code>&lt;value&gt;</code></td>
<td>Tenable.sc Director checks all certificates in a chain against the CRL.</td>
</tr>
<tr>
<td>chain</td>
<td>Tenable.sc Director checks only the end-entity certificate in a chain against the CRL.</td>
</tr>
<tr>
<td>leaf</td>
<td>Tenable.sc Director checks only the end-entity certificate in a chain against the CRL.</td>
</tr>
<tr>
<td>SSLCARevocationFile <code>&lt;filepath&gt;</code></td>
<td>Specifies the file path for the CRL file in Tenable.sc Director. For example, <code>/opt/sc/support/conf/crl/ca.crl</code>.</td>
</tr>
</tbody>
</table>

   b. Save the file.

   Tenable.sc Director saves your configuration.

9. Run the following command to create a symbolic link for the CRL file:

   ```
   $ ln -s <crl parameter value in the YourCAname.conf file> `openssl crl -hash -noout -in <crl parameter value in the YourCAname.conf file>` .r0
   ```

   For example:

   ```
   $ ln -s /opt/sc/support/conf/crl/ca.crl `openssl crl -hash -noout -in /opt/sc/support/conf/crl/ca.crl` .r0
   ```
**Caution:** Do not use a single quote character (’) instead of a backtick character (‘); this command requires the backtick.

Tenable.sc Director creates a symbolic link for the CRL file.

10. Restart Tenable.sc Director, as described in [Start, Stop, or Restart Tenable.sc Director](#).

Tenable.sc Director restarts.
Configure OCSP Validation in Tenable.sc Director

**Required User Role:** Root user

You can configure Online Certificate Status Protocol (OCSP) validation in Tenable.sc Director to prevent users from authenticating to Tenable.sc Director if their certificate matches a revocation on your OCSP server.

**Note:** Tenable Support does not assist with OCSP configuration in Tenable.sc Director.

Before you begin:

- Confirm that you have an OCSP server configured in your environment.

To configure OCSP validation in Tenable.sc Director:

1. In a text editor, open the `/opt/sc/support/conf/sslverify.conf` file.
   
   a. Set the `SSLVerifyClient` setting to `Require` or `Optional`, as described in `SSLVerifyClient`.
   
   b. Set the `SSLVerifyDepth` setting, as described in `SSLVerifyDepth`.
   
   c. Save the file.

   Tenable.sc Director saves your configuration.

2. In a text editor, open the `/opt/sc/support/conf/vhostssl.conf` file.
   
   a. Add the following content at the end of the file:

   ```
   SSLOCSPEnable on
   SSLOCSPDefaultResponder <URI>
   SSLOCSPOverrideResponder on
   ```

   Where `<URI>` is the URI for your OCSP server.
   
   b. Save the file.

   Tenable.sc Director saves your configuration.

3. Restart Tenable.sc Director, as described in [Start, Stop, or Restart Tenable.sc Director](#).

   Tenable.sc Director restarts.
Certificates and Certificate Authorities in Tenable.sc Director

Tenable.sc Director includes the following defaults:

- a default Tenable.sc server certificate (SecurityCenter.crt)
- a Tenable.sc certificate authority (CA), which signs SecurityCenter.crt
- a DigiCert High Assurance EV Root CA

However, you may want to upload your own CAs or certificates for advanced configurations or to resolve scanning issues. For more information, see:

- [Tenable.sc Director Server Certificates](#)
- [Trust a Custom CA](#)
- [Certificate Authentication](#)
- [Custom Plugin Packages for NASL and CA Certificate Upload](#)
- [Manual Nessus SSL Certificate Exchange](#)
Tenable.sc Director Server Certificates

Tenable.sc Director ships with a default Tenable.sc Director server certificate and key: SecurityCenter.crt and SecurityCenter.key. In some cases, you must replace it or regenerate it.

If you replace the server certificate with a self-signed certificate, you may need to upload the CA for your server certificate to Nessus or your browser.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The default certificate for Tenable.sc Director is untrusted.</td>
<td>Upload a certificate for the Tenable.sc Director server, as described in <a href="#">Upload a Server Certificate for Tenable.sc</a>. If the new server certificate is self-signed, plugin 51192 may report that the Tenable.sc Director server certificate is untrusted. To configure Nessus to trust the server certificate, upload the CA certificate to Nessus.</td>
</tr>
<tr>
<td>Your browser reports that the Tenable.sc Director server certificate is untrusted.</td>
<td>Upload a CA certificate for the Tenable.sc Director server certificate to your browser.</td>
</tr>
<tr>
<td>Plugin 51192 reports that the Tenable.sc Director server certificate expired.</td>
<td>Regenerate the Tenable.sc Director server certificate, as described in <a href="#">Regenerate the Tenable.sc Director Server Certificate</a>.</td>
</tr>
</tbody>
</table>
Upload a Server Certificate for Tenable.sc

**Required User Role:** Root user

For information about Tenable.sc Director server certificates, see [Tenable.sc Director Server Certificates](#).

**Tip:** The custom certificate email address must not be SecurityCenter@SecurityCenter or subsequent upgrades cannot retain the new certificate.

Before you begin:

- Save your new server certificate and key files as host.crt and host.key.

To upload a server certificate for Tenable.sc Director:

1. Log in to Tenable.sc Director via the user interface.

2. Back up the existing SecurityCenter.crt and SecurityCenter.key files located in the `/opt/sc/support/conf` directory.

   For example:

   ```
   # cp /opt/sc/support/conf/SecurityCenter.crt /tmp/SecurityCenter.crt.bak
   # cp /opt/sc/support/conf/SecurityCenter.key /tmp/SecurityCenter.key.bak
   ```

3. To rename the host.crt and host.key files and copy them to the `/opt/sc/support/conf` directory, run:

   ```
   # cp host.crt /opt/sc/support/conf/SecurityCenter.crt
   # cp host.key /opt/sc/support/conf/SecurityCenter.key
   ```

   If prompted, type y to overwrite the existing files.

4. To confirm the files have the correct permissions (640) and ownership (tns), run:
Note: If an intermediate certificate is required, it must also be copied to the system and given the correct permissions (640) and ownership (tns). Additionally, you must remove the # from the line in /opt/sc/support/conf/vhostssl.conf that begins with #SSLCertificateChainFile to enable the setting. Modify the path and filename to match the uploaded certificate.

If necessary, change the ownership or permissions.

a. To change the ownership, run:

```bash
# chown tns:tns /opt/sc/support/conf/SecurityCenter.crt

# chown tns:tns /opt/sc/support/conf/SecurityCenter.key
```

b. To change the permissions, run:

```bash
# chmod 640 /opt/sc/support/conf/SecurityCenter.crt

# chmod 640 /opt/sc/support/conf/SecurityCenter.key
```

5. Restart the Tenable.sc Director service:

```bash
# service SecurityCenter restart
```

6. In a browser, log in to the Tenable.sc Director user interface as a user with administrator permissions.

7. When prompted, verify the new certificate details.

What to do next:
If you uploaded a self-signed server certificate and plugin 51192 reports that the CA for your self-signed certificate is untrusted, upload the custom CA certificate to Nessus.
Regenerate the Tenable.sc Director Server Certificate

Required User Role: tns user

Tenable.sc Director ships with a default server certificate that is valid for two years. After the certificate expires, you must regenerate the SSL certificate.

To regenerate the Tenable.sc Director SSL certificate:

1. Log in to Tenable.sc Director via the user interface.
2. Run the following command:

   `/opt/sc/support/bin/php /opt/sc/src/tools/installSSLCertificate.php`

(Optional) If you want to suppress the self-signed warning or specify a Common Name, include an optional argument.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-q</td>
<td>Suppresses the warning: This script generates a self-signed SSL certificate, which is not recommended for production.</td>
</tr>
<tr>
<td>-h &lt;IP</td>
<td>hostname&gt;</td>
</tr>
</tbody>
</table>

Tenable.sc Director generates a new certificate.

3. Restart the Tenable.sc Director service:

   `# service SecurityCenter restart`

   The service restarts and Tenable.sc Director applies the new certificate.
Trust a Custom CA

**Required User Role:** Root user

You can configure Tenable.sc Director to trust a custom CA for certificate authentication or other uses.

To configure Tenable.sc Director to trust a custom CA:

1. Log in to Tenable.sc Director via the user interface.
2. Copy the required PEM-encoded CA certificate (and intermediate CA certificate, if needed) to the Tenable.sc Director server's /tmp directory.
   
   In this example, the file is named ROOTCA2.cer.
3. Run the `installCA.php` script to create the required files for each CA in `/opt/sc/data/CA`:
   
   ```
   # /opt/sc/support/bin/php /opt/sc/src/tools/installCA.php /tmp/ROOTCA2.cer
   ```

   Tenable.sc Director processes all the CAs in the file.
4. Restart Tenable.sc Director, as described in Start, Stop, or Restart Tenable.sc Director.
System Settings

The **System** and **Username** menus in the top navigation bar contain several options to configure Tenable.sc Director system settings. Administrator users can configure more options than organizational users.

- [Configuration Settings](#)
- Lumin Data
- [Diagnostics Settings](#)
- [Job Queue Events](#)
- [System Logs](#)
- [Publishing Sites Settings](#)
- [Keys Settings](#)
- [Username Menu Settings](#)
Configuration Settings

The configuration menu includes the following settings:

- Data Expiration Settings
- External Schedules Settings
- Mail Settings
- Miscellaneous Settings
- License Settings
- Plugins/Feed Settings
- SAML Settings
- Security Settings

Data Expiration Settings

Data expiration determines how long Tenable.sc retains acquired data.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Data Lifetime</td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td>The number of days you want Tenable.sc to retain active or agent scan vulnerability data stored in IP repositories. The default value of this option is 365 days.</td>
</tr>
<tr>
<td>Passive</td>
<td>The number of days you want Tenable.sc to retain NNM vulnerability data stored in IP repositories. The default value of this option is 7 days.</td>
</tr>
<tr>
<td>Event</td>
<td>The number of days you want Tenable.sc to retain LCE event data stored in IP repositories. The default value of this option is 365 days.</td>
</tr>
<tr>
<td>Compliance</td>
<td>The number of days you want Tenable.sc to retain audit compliance data stored in IP repositories. The default value of this option is 365 days.</td>
</tr>
<tr>
<td>Mitigated</td>
<td>The number of days you want Tenable.sc to retain mitigated vulnerability data. The default value of this option is 365 days.</td>
</tr>
<tr>
<td>Agent</td>
<td>The number of days you want Tenable.sc to retain agent scan vulnerability data</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Generated Object Lifetime</td>
<td></td>
</tr>
<tr>
<td>Closed Tickets</td>
<td>The number of days you want Tenable.sc to retain closed tickets. The default value of this option is 365 days.</td>
</tr>
<tr>
<td>Scan Results</td>
<td>The number of days you want Tenable.sc to retain scan results. The default value of this option is 365 days.</td>
</tr>
<tr>
<td>Report Results</td>
<td>The number of days you want Tenable.sc to retain report results. The default value of this option is 365 days.</td>
</tr>
<tr>
<td>Tenable.sc Instance Data Lifetime</td>
<td></td>
</tr>
<tr>
<td>Scan Results</td>
<td>The number of days you want Tenable.sc Director to retain scan results imported from managed Tenable.sc instances. You can manually re-retrieve scan result data from managed Tenable.sc instances after the data has been removed from Tenable.sc Director. The default value of this option is 30 days.</td>
</tr>
</tbody>
</table>

**External Schedules Settings**

The Tenable.sc external schedule settings are used to determine the update schedule for the common tasks of pulling NNM data, IDS signature updates, and IDS correlation updates.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nessus Network Monitor</td>
<td></td>
</tr>
<tr>
<td>Pull Interval</td>
<td>This option configures the interval that Tenable.sc will use to pull results from the attached NNM instances. The default setting is 1 hour. The timing is based from the start of the Tenable.sc service on the host system.</td>
</tr>
<tr>
<td>Log Correlation Engine</td>
<td></td>
</tr>
<tr>
<td>IDS Signatures</td>
<td>Frequency to update Tenable.sc IDS signatures via third-party sources. The schedule is shown along with the time zone being used.</td>
</tr>
<tr>
<td>IDS Correlation Databases</td>
<td>Frequency to push vulnerability information to the LCE for correlation. The schedule is shown along with the time zone being used.</td>
</tr>
</tbody>
</table>
Each of the update schedule times may also be configured to occur by time in a particular time zone, which can be selected via the Time Zone link next to each hour selection.

Mail Settings

The Mail option designates SMTP settings for all email related functions of Tenable.sc. Available options include SMTP host, port, authentication method, encryption, and return address. In addition, a Test SMTP Settings link is displayed in the top left of the page to confirm the validity of the settings.

**Note:** The Return Address defaults to noreply@localhost. Use a valid return email address for this option. If this option is empty or the email server requires emails from valid accounts, the email will not be sent by the email server.

**Note:** Type the Username in a format supported by your SMTP server (for example, username@domain.com or domain\username).

Miscellaneous Settings

The Miscellaneous Configuration section offers options to configure settings for web proxy, syslog, notifications, and enable or disable a variety of reporting types that are encountered and needed only in specific situations.

Web Proxy

From this configuration page, a web proxy can be configured by entering the host URL (proxy host-name or IP address), port, authentication type, username, and password. The host name used must resolve properly from the Tenable.sc host.

Syslog

The Syslog section allows for the configuration and sending of Tenable.sc log events to the local syslog service. When Enable Forwarding is enabled, the forwarding options are made available for selection. The Facility option provides the ability to enter the desired facility that will receive the log messages. The Severity option determines which level(s) of syslog messages will be sent: Informational, Warning, and/or Critical.

Scanning
The **IP Randomization** option specifies how you want Tenable.sc to send active scan target lists to Nessus and Tenable.io scanners.

You enable or disable IP randomization for all configured active scans; you cannot configure IP randomization on a per-scan basis.

- When enabled, Tenable.sc randomizes the targets in the active scan before sending the target list to the scanners to reduce strain on network devices during large active scans.

<table>
<thead>
<tr>
<th>Scan</th>
<th>Randomization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000 or fewer targets</td>
<td>Tenable.sc randomizes all the IP addresses in the target list.</td>
</tr>
<tr>
<td>1,001 or more targets</td>
<td>Tenable.sc randomizes all the IP addresses in the target list by:</td>
</tr>
<tr>
<td></td>
<td>1. Ordering the IP addresses numerically and splitting them into 100 groups.</td>
</tr>
<tr>
<td></td>
<td>2. Randomly selecting a group and choosing the lowest IP address from that group.</td>
</tr>
<tr>
<td></td>
<td>3. Selecting groups and IP addresses until all IP addresses in all groups are randomized in the target list.</td>
</tr>
</tbody>
</table>

If the active scan includes a Tenable.io scanner, Tenable.sc breaks the target list into smaller lists (256 IP addresses each) before sending to Tenable.io.

**Note:** Some randomized target lists (such as very small target lists) may still contain sequences of increasing IP addresses. This is a possible outcome of randomization, not an indication that randomization failed.

- When disabled, Tenable.sc organizes the target list by increasing IP address. Then, scanners scan targets, starting with the lowest IP address and finishing with the highest IP address.

**Tip:** The **Max simultaneous hosts per scan** scan policy option specifies how many IP addresses Tenable.sc sends to each scanner at a time. For more information, see Scan Policy Options.

**Notifications**

The **Notifications** section defines the Tenable.sc web address used when notifications are generated for alerts and tickets.

**Report Generation**

---

Copyright © 2020 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.
Among the reporting standards for the Defense Information Systems Agency (DISA) are the Assessment Summary Results (ASR), Assessment Results Format (ARF), and Consolidated Assessment Results Format (CARF) styles. Additionally, CyberScope reports utilize Lightweight Asset Summary Results Schema (LASR) style reports, which are used by some segments of governments and industry. These formats are typically used only by select groups and organizations for specific needs that do not apply to many organizations.

To allow users to choose these reports during report creation, you must enable the Enable DISA ARF, Enable DISA Consolidated ARF, Enable DISA ASR, and Enable CyberScope toggles. For more information, see Reports.

Privacy

The Enable Usage Statistics option specifies whether Tenable collects anonymous telemetry data about your Tenable.sc deployment.

When enabled, Tenable collects usage statistics that cannot be attributed to a specific user or customer. Tenable does not collect personal data or personally identifying information (PII).

Usage statistics include, but are not limited to, data about your visited pages, your used reports and dashboards, your Tenable.sc license, and your configured features. Tenable uses the data to improve your user experience in future Tenable.sc releases. You can disable this option at any time to stop sharing usage statistics with Tenable.

After you enable or disable this option, all Tenable.sc users must refresh their browser window for the changes to take effect.

License Settings

The License Configuration section allows you to configure licensing and activation code settings for Tenable.sc and all attached Tenable products.

For information about the Tenable.sc license count, see License Requirements. To add or update a license, see Apply a New License or Update an Existing License.

Plugins/Feed Settings

The Plugins/Feed Configuration page displays the Plugin Detail Locale for Tenable.sc and the feed and plugin update (scanner update) schedules.

For more information, see Edit Plugin and Feed Settings and Schedules.
### Update Description

<table>
<thead>
<tr>
<th>Update</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable.sc</td>
<td>Retrieves the latest Tenable.sc feed from Tenable. This feed includes data for general use, including templates (e.g., dashboards, ARCs, reports, policies, assets, and audit files), template-required objects, some general plugin information, and updated VPR values.</td>
</tr>
<tr>
<td>Active Plugins</td>
<td>Retrieves the latest active plugins feed (for Nessus and Tenable.io scanners) from Tenable. Tenable.sc pushes the feed to Nessus and Tenable.io scanners.</td>
</tr>
<tr>
<td>Passive Plugins</td>
<td>Retrieves the latest passive plugins feed from Tenable. Tenable.sc pushes the feed to NNM instances.</td>
</tr>
<tr>
<td>Event Plugins</td>
<td>Retrieves the latest event plugins feed from Tenable. Tenable.sc uses the feed locally with LCE data but does not push the feed to LCE; LCE retrieves the feed directly from Tenable.</td>
</tr>
</tbody>
</table>

For information about Tenable.sc-Tenable plugins server communications encryption, see [Encryption Strength](#).

### Plugin Detail Locale

The local language plugin feature allows you to display portions of plugin data in local languages. When available, translated text displays on all pages where plugin details are displayed.

Select **Default** to display plugin data in English.

Tenable.sc cannot translate text within custom files. You must upload a translated **Active Plugins.xml** file in order to display the file content in a local language.

For more information, see [Configure Plugin Text Translation](#).

### Schedules

Tenable.sc automatically updates Tenable.sc feeds, active plugins, passive plugins, and event plugins. If you upload a custom feed or plugin file, the system merges the custom file data with the data contained in the associated automatically updating feed or plugin.

You can upload `.tar.gz` files with a maximum size of 1500 MB.

For more information, see [Edit Plugin and Feed Settings and Schedules](#).

### SAML Settings
Use the SAML section to configure SAML 2.0 or Shibboleth 1.3-based SAML authentication for Tenable.sc users. For more information, see SAML Authentication.

Security Settings

Use the Security section to define the Tenable.sc web interface login parameters and options for account logins. You can also configure banners, headers, and classification headers and footers.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Settings</td>
<td></td>
</tr>
<tr>
<td>Session Timeout</td>
<td>The web session timeout in minutes (default: 60).</td>
</tr>
<tr>
<td>Maximum Login Attempts</td>
<td>The maximum number of user login attempts allowed by Tenable.sc before the account is locked out (default: 20). Setting this value to 0 disables this feature.</td>
</tr>
<tr>
<td>Minimum Password Length</td>
<td>This setting defines the minimum number of characters for passwords of accounts created using the local TNS authentication access (default: 3).</td>
</tr>
<tr>
<td>Password Complexity</td>
<td>When enabled, user passwords must be at least 4 characters long and contain at least one of each of the following:</td>
</tr>
<tr>
<td></td>
<td>- An uppercase letter</td>
</tr>
<tr>
<td></td>
<td>- A lowercase letter</td>
</tr>
<tr>
<td></td>
<td>- A numerical character</td>
</tr>
<tr>
<td></td>
<td>- A special character</td>
</tr>
<tr>
<td>Note:</td>
<td>After you enable Password Complexity, Tenable.sc prompts all users to reset their passwords the next time they log in to Tenable.sc.</td>
</tr>
<tr>
<td>Note:</td>
<td>If you enable Password Complexity and set the Minimum Password Length to a value greater than 4, Tenable.sc enforces the longer password requirement.</td>
</tr>
<tr>
<td>Startup Banner Text</td>
<td>Type the text banner that is displayed prior to the login interface.</td>
</tr>
<tr>
<td>Header Text</td>
<td>Adds custom text to the top of the Tenable.sc user interface pages. The text may be used to identify the company, group, or other organizational inform-</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Classification Type   | Adds a header and footer banner to Tenable.sc to indicate the classification of the data accessible via the software. Current options are **None**, **Unclassified**, **Confidential**, **Secret**, **Top Secret**, and **Top Secret – No Foreign**. Sample header:  
|                       | ![Sample Header](image1.png)                                                                                                                     |
|                       | Sample footer:  
<p>|                       | <img src="image2.png" alt="Sample Footer" />                                                                                                                   |
| Allow API Keys        | When enabled, allows users to generate API keys as an authentication method for Tenable.sc API requests. For more information, see <strong>Enable API Key Authentication</strong>. |
| Allow Session Management | This setting is disabled by default. When enabled, the <strong>Session Limit</strong> option will appear. This feature displays the option that will allow the administrator user to set a session limit for all users. |
| Disable Inactive      | When enabled, Tenable.sc disables user accounts after a set period of inactivity.                                                               |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>A disabled user cannot log in to Tenable.sc, but other users can use and manage objects owned by the disabled user.</td>
</tr>
<tr>
<td>Days Users Remain Enabled</td>
<td>When <strong>Disable Inactive Users</strong> is enabled, specifies the number of inactive days you want to allow before automatically disabling a user account.</td>
</tr>
<tr>
<td>Session Limit</td>
<td>Any number entered here will be saved as the maximum number of sessions a user can have open at one time. If you log in and the session limit has already been reached, you will be prompted with a warning that the oldest session with that username will be logged out automatically. You can cancel the login, or proceed with the login and end the oldest session.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This behavior is different for CAC logins. The previously described behavior is bypassed as was the old login behavior.</td>
</tr>
<tr>
<td>Login Notifications</td>
<td>Sends notifications for each time a user logs in.</td>
</tr>
<tr>
<td>WebSeal</td>
<td>Allows you to enable or disable WebSEAL. WebSEAL supports multiple authentication methods, provides Security Access Authorization service, and single sign on capabilities.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution:</strong> It is strongly advised that the user confirm, in a separate session, that at least one user (preferably an administrator user) is able to log-in successfully via WebSEAL before the user that enabled WebSEAL logs out. Otherwise, if there is an issue, no one will be able to access Tenable.sc to turn WebSEAL off.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution:</strong> Any user created while WebSEAL was enabled will <strong>not</strong> have a password and an admin must update the user account to establish a password. Any user that existed before the enabling of WebSEAL must revert to their old password.</td>
</tr>
<tr>
<td>PHP Serialization</td>
<td></td>
</tr>
<tr>
<td>Operational Status</td>
<td>Summarizes your current setting.</td>
</tr>
<tr>
<td>PHP Serialization</td>
<td>Specifies whether you want to allow or prevent PHP serialization in</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mode</td>
<td>Tenable.sc.</td>
</tr>
<tr>
<td></td>
<td>• <strong>PHP Serialization ON</strong> — Tenable.sc performs PHP serialization and Tenable.sc features operate as expected.</td>
</tr>
<tr>
<td></td>
<td>• <strong>PHP Serialization OFF</strong> — Tenable.sc does not perform PHP serialization and prevents users from importing or exporting the following objects.</td>
</tr>
<tr>
<td></td>
<td>• Assets</td>
</tr>
<tr>
<td></td>
<td>• Scan policies</td>
</tr>
<tr>
<td></td>
<td>• Assurance Report Cards</td>
</tr>
<tr>
<td></td>
<td>• Reports</td>
</tr>
<tr>
<td></td>
<td>• Audit files</td>
</tr>
<tr>
<td></td>
<td>• Dashboards</td>
</tr>
</tbody>
</table>
Edit Plugin and Feed Settings and Schedules

**Required User Role:** Administrator or organizational user with appropriate permissions. For more information, see [User Roles](#).

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

To view and edit plugin and feed settings and schedules as an administrator user:

1. Log in to Tenable.sc Director via the user interface.
2. In the top navigation bar, click **System > Configuration**.
   The **Configuration** page appears.
3. Click the **Plugins/Feed** button.
   The **Plugins/Feed Configuration** page appears.
4. View the **Plugin Detail Locale** section to see the local language configured for Tenable.sc Director.
5. Expand the **Schedules** section to show the settings for the **Tenable.sc Feed**, **Active Plugins**, **Passive Plugins**, or **Event Plugins** schedule.
6. If you want to update a plugin or feed on demand, click **Update**. You cannot update feeds with invalid activation codes.
7. If you want to upload a custom feed file, click **Choose File**.
8. Click **Submit**.
   Tenable.sc Director saves your configuration.

To view and edit plugin and feed settings and schedules as an organizational user:

1. Log in to Tenable.sc Director via the user interface.
2. In the top navigation bar, click **Username > Feeds**.
   The Plugins/Feed Configuration page appears.
3. View the **Plugin Detail Locale** section to see the local language configured for Tenable.sc Director.
4. Expand the **Schedules** section to show the settings for the **Tenable.sc Feed, Active Plugins, Passive Plugins**, or **Event Plugins** schedule.

5. If you want to update a plugin or feed on demand, click **Update**. You cannot update feeds with invalid activation codes.

6. If you want to upload a custom feed file, click **Choose File**.

7. Click **Submit**.
   Tenable.sc Director saves your configuration.
Configure Plugin Text Translation

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

To configure plugin text translation:

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **System > Configuration**.
3. Click the **Plugins/Feed** button.
4. If you want plugin text to display in a local language, select a language from the **Locale List** box.
5. Click **Apply**.
6. Perform an on-demand **Active Plugins** update to obtain available translations.
API Key Authentication

You can enable API key authentication to allow users to use API keys as an authentication method for Tenable.sc API requests. Without API keys, users must use the /token endpoint to log in to the Tenable.sc API and establish a token for subsequent requests, as described in Token in the Tenable.sc API Guide.

Tenable.sc attributes actions performed with API keys to the user account associated with the API keys. You can only perform actions allowed by the privileges granted to the user account associated with the API keys.

You must enable the Allow API Keys toggle in your Security Settings to allow users to perform API key authentication. Then, users can generate API keys for themselves or for other users. API keys include an access key and secret key that must be used together for API key authentication. For more information, see Enable API Key Authentication and Generate API Keys.

A user's API keys can be used for Tenable.sc API request authentication by including the x-apikey header element in your HTTP request messages, as described in API Key Authorization in the Tenable.sc API Best Practices Guide.

Deleting API keys prevents users from authenticating Tenable.sc API requests with the deleted keys. For more information, see Delete API Keys.

For more information about the Tenable.sc API, see the Tenable.sc API Guide and the Tenable.sc API Best Practices Guide.
Enable API Key Authentication

**Required User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

You can enable API key authentication to allow users to use API keys as an authentication method for Tenable.sc API requests. For more information, see API Key Authentication.

To allow users to authenticate to the Tenable.sc API using API keys:

1. Log in to Tenable.sc Director via the user interface.
2. In the top navigation bar, click System > Configuration.
   
   The Configuration page appears.
3. Click the Security tile.
   
   The Security Configuration page appears.
4. In the Authentication Settings section, click Allow API Keys to enable the toggle.
5. Click Submit.

   Tenable.sc Director saves your configuration.

What to do next:

- Generate API keys for a user, as described in Generate API Keys.
Disable API Key Authentication

**Required User Role:** Administrator or organizational user with appropriate permissions. For more information, see [User Roles](#).

**Caution:** Disabling API keys prevents users from authenticating API requests with API keys. Disabling API keys does not delete existing API keys. If you re-enable API keys, Tenable.sc reauthorizes any API keys they were active before you disabled API key authentication.

For more information, see [API Key Authentication](#).

To disable API key authentication:

1. Log in to Tenable.sc Director via the user interface.
2. In the top navigation bar, click **System > Configuration**.
   
   The **Configuration** page appears.
3. Click the **Security** tile.
   
   The **Security Configuration** page appears.
4. In the **Authentication Settings** section, click **Allow API Keys** to disable the toggle.
5. Click **Submit**.
   
   Tenable.sc Director saves your configuration.
Diagnostics Settings

This page displays and creates information that assists in troubleshooting issues that may arise while using Tenable.sc Director.

System Status

You can use this section to view the current status of system functions.

<table>
<thead>
<tr>
<th>System Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct Java Version</td>
<td>Indicates whether the minimum version of Java required to support Tenable.sc Director functionality is installed.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <a href="#">Before You Upgrade</a>.</td>
</tr>
<tr>
<td>Sufficient Disk Space</td>
<td>Indicates whether you have enough disk space to support Tenable.sc Director functionality. A red X indicates the disk is at 95% capacity or higher.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <a href="#">Hardware Requirements</a>.</td>
</tr>
<tr>
<td>Correct RPM Package Installed</td>
<td>Indicates whether you have the correct Tenable.sc Director RPM installed for your operating system.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <a href="#">System Requirements</a>.</td>
</tr>
<tr>
<td>Touch Debugging</td>
<td>Indicates whether touch debugging is enabled. You may experience performance and storage issues if you leave touch debugging enabled for extended periods of time.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <a href="#">Diagnostics Settings</a>.</td>
</tr>
<tr>
<td>Migration Errors</td>
<td>Indicates whether an error occurred during a recent Tenable.sc Director update.</td>
</tr>
</tbody>
</table>

Diagnostics File

You can use this section to generate a diagnostics file for troubleshooting with Tenable Support. For more information, see [Generate a Diagnostics File](#).
Generate a Diagnostics File

**Required User Role:** Administrator

To generate a diagnostics file for Tenable Support:

1. Log in to Tenable.sc Director via the user interface.

2. In the top navigation bar, click **System > Diagnostics**.
   
   The **Diagnostics** page appears.

3. In the **Diagnostics File** section, click **Create Diagnostics File**.
   
   The page updates with options to configure the diagnostics file.

4. In the **General** section, if you want to omit IP addresses from the diagnostics file, click to enable the **Strip IPs from Chapters** toggle.

5. In the **Chapters** section, click the toggles to enable or disable the chapters you want to include in the diagnostics file.

6. Click **Generate File**.
   
   The system generates a `debug.zip` file and saves it in `/opt/sc`.

**What to do next:**

- Share the `debug.zip` file with Tenable Support for troubleshooting.
Enable Touch Debugging

**Required User Role:** Administrator

You can enable touch debugging to generate logs for troubleshooting with Tenable Support.

To enable touch debugging:

1. Log in to Tenable.sc Director via the user interface.
2. In the top navigation bar, click System > Diagnostics.
   
   The Diagnostics page appears.
3. In the Touch Debugging section, select one or more touch debug files Tenable Support asked you to enable.
4. Click Enable/Disable Touch Debugging.
   
   Tenable.sc Director enables the touch debug files you selected and saves one or more log files to /opt/sc/admin/logs.

What to do next:

- Share the files with Tenable Support.
- Disable any unneeded touch debug files, as described in Disable Touch Debugging.

**Note:** Tenable does not recommend leaving touch debug files enabled on Tenable.sc Director after you send the log files to Tenable Support. You may experience performance and storage issues if you leave touch debugging enabled for extended periods of time.
Disable Touch Debugging

Required User Role: Administrator

Tenable does not recommend leaving touch debug files enabled on Tenable.sc Director after you send the log files to Tenable Support. You may experience performance and storage issues if you leave touch debugging enabled for extended periods of time.

For more information about touch debugging files, see Diagnostics Settings.

To disable touch debugging:

1. Log in to Tenable.sc Director via the user interface.

2. In the top navigation bar, click System > Diagnostics.

   The Diagnostics page appears.

3. In the Touch Debugging section:
   - To remove individual touch debug files, deselect the files.
   - To remove all touch debug files, click Deselect All.

4. Click Enable/Disable Touch Debugging.

   Tenable.sc Director disables the touch debugging files you deselected.

What to do next:

- Follow Tenable Support’s instructions to manually remove old log files from /opt/sc/admin/logs.
Job Queue Events

Path: **System > Job Queue**

Job Queue is a Tenable.sc Director feature that displays specified events in a list for review.

You can view and sort Job Queue notifications in several ways by clicking on the desired sort column. Using the ⌁ menu next to an item, that item may be viewed for more detail or, if the job is running, the process may be killed. Killing a process should be done only as a last resort, as killing a process may have undesirable effects on other Tenable.sc Director processes.
System Logs

Tenable.sc Director logs contain detailed information about functionality to troubleshoot unusual system or user activity. You can use the system logs for debugging and for maintaining an audit trail of users who access Tenable.sc Director or perform basic functions (for example, changing passwords).

For more information, see View System Logs.
View System Logs

Required User Role: Administrator or organizational user with appropriate permissions. For more information, see User Roles.

For more information, see System Logs.

To view system logs:

1. Log in to Tenable.sc Director via the user interface.

2. Click System > System Logs (Administrator users) or Username > System Logs (Organizational users).

   The System Logs page appears.

3. To filter the logs, see Apply a Filter.

   The page updates to reflect the filter you applied.
Publishing Sites Settings

Path: System > Publishing Sites

Organizations may configure publishing sites as targets to send report results to a properly configured web server or a Defense Information Systems Agency (DISA) Continuous Monitoring and Risk Scoring (CMRS) site.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name for the publishing site.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a description of the publishing site.</td>
</tr>
<tr>
<td>Type</td>
<td>The method Tenable.sc Director uses to publish to the site. Available options are HTTP Post or CMRS. Use the selection appropriate for the configuration of the publishing site.</td>
</tr>
<tr>
<td>Max Chunk Size (MB)</td>
<td>If the target is a CMRS site, Tenable sends the report in chunks sized according to this value.</td>
</tr>
<tr>
<td>URI</td>
<td>The target address to send the report to when completed.</td>
</tr>
<tr>
<td>Authentication</td>
<td>There are two methods of authentication available: SSL Certificate and Password.</td>
</tr>
<tr>
<td>Username / Password</td>
<td>If you select Password as the Authentication method, the credentials to authenticate to the target publishing server.</td>
</tr>
<tr>
<td>Certificate</td>
<td>If you selected SSL Certificate as the Authentication method, the certificate you want to use for authentication.</td>
</tr>
<tr>
<td>Organizations</td>
<td>Select the organization(s) that are allowed to publish to the configured site.</td>
</tr>
<tr>
<td>Verify Host</td>
<td>When enabled, Tenable.sc Director verifies that the target address specified in the URI option matches the CommonName (CN) in the SSL certificate from the target publishing server.</td>
</tr>
</tbody>
</table>
Keys Settings

Keys allow administrator users to use key-based authentication with a remote Tenable.sc (remote repository) or between a Tenable.sc and an LCE server. This also removes the need for Tenable.sc administrators to know the administrator login or password of the remote system.

**Note:** The public key from the local Tenable.sc must be added to the Keys section of the Tenable.sc from which you wish to retrieve a repository. If the keys are not added properly, the remote repository add process prompts for the root username and password of the remote host to perform a key exchange before the repository add/sync occurs.

For more information, see Add a Key, Delete a Key, and Download the Tenable.sc Director SSH Key.

Remote LCE Key Exchange

A manual key exchange between the Tenable.sc and the LCE is normally not required; however, in some cases where remote root login is prohibited or key exchange debugging is required, you must manually exchange the keys.

For the remote LCE to recognize the Tenable.sc, you need to copy the SSH public key of the Tenable.sc and append it to the /opt/lce/.ssh/authorized_keys file. The /opt/lce/daemons/lce-install-key.sh script performs this function. For more information, see Manual LCE Key Exchange.
Add a Key

**Required User Role:** Administrator

For more information, see [Keys Settings](#).

To add a new key:

1. Log in to Tenable.sc via the user interface.
2. Click **System > Keys**.
   
The **Keys** page appears.
3. Click **Add**.
4. In the **Type** drop-down, select **DSA** or **RSA**.
5. (Optional) In the **Command** box, add a description or note about the key.
6. In the **Public Key** box, type the text of your public key from your remote Tenable.sc.
7. Click **Submit**.
   
   Tenable.sc Director saves your configuration.
Delete a Key

**Required User Role:** Administrator

For more information, see [Keys Settings](#).

To delete a key:

1. Log in to Tenable.sc Director via the user interface.
2. Click **System > Keys**.
3. In the row for the key you want to delete, click the menu.
   The actions menu appears.
4. Click **Delete**.
   A confirmation window appears.
5. Click **Delete**.
Download the Tenable.sc Director SSH Key

**Required User Role:** Administrator

For more information, see [Keys Settings](#).

To download the Tenable.sc Director SSH key:

1. Log in to Tenable.sc Director via the user interface.
2. Click **System > Keys**.
3. In the **Options** drop-down, click **Download SC Key**.

   The Tenable.sc Director SSH key downloads.
Username Menu Settings

The username menu in the top navigation bar contains pages to manage your user account.

**Note:** Depending on the screen resolution, the username may be omitted and only a user icon appears.

About

Path: **Username > About**

The **About** menu item displays the Tenable.sc Director version, Server Build ID, and copyright information.

System Logs (Organizational Users Only)

Path: **Username > System Logs**

For a complete discussion about system logs, see **System Logs**.

Profile (Organizational Users Only)

Path: **Username > Profile**

The **Profile** option launches the **Edit User Profile** page, where you can modify some of your user account information and permissions. For more information about user account options, see **User Accounts**.

Feeds (Organizational Users Only)

Path: **Username > Feeds**

The **Feeds** option displays information about the Tenable.sc Director feeds and plugin sets and, if permitted, a link to update the plugins either through Tenable.sc Director or by manually uploading plugins. The displayed feeds are for Tenable.sc Feed, Active Plugins, Passive Plugins, and Event Plugins. Only feeds with valid Activation Codes are updatable.

Plugins are scripts used by the Nessus, NNM, and LCE servers to interpret vulnerability data. For ease of operation, Nessus and NNM plugins are managed centrally by Tenable.sc Director and pushed out to their respective scanners. LCE servers download their own event plugins and Tenable.sc downloads...
event plugins for its local reference. Tenable.sc Director does not currently push event plugins to LCE servers.

For more information about plugin/feed settings, see Configuration Settings and Edit Plugin and Feed Settings and Schedules.

Notifications

Path: Username > Notifications

Notifications are a feature of Tenable.sc Director that allow specified events to display a pop-up in the lower right-hand corner of the Tenable.sc Director user interface.

Current notifications can be viewed by clicking on the notifications menu item.

Plugins

Path: Username > Plugins

Plugins are scripts used by the Nessus, NNM, and LCE servers to interpret vulnerability data. For ease of operation, Nessus and NNM plugins are managed centrally by Tenable.sc and pushed out to their respective scanners. LCE servers download their own event plugins and Tenable.sc downloads event plugins for its local reference. Tenable.sc does not currently push event plugins to LCE servers.

Within the Plugins interface, click the information icon next to the Plugin ID and search for specific plugins utilizing the filtering tools to view plugin details/source.

For more information about custom plugins, see Custom Plugin Packages for NASL and CA Certificate Upload.

Help

Path: Username > Help

The Help option opens the Tenable.sc Director User Guide section for your page. To access other Tenable documentation, see https://docs.tenable.com/.

Logout

To end your session in Tenable.sc Director, click Username > Logout. Tenable recommends closing your browser window after logging out.
Custom Plugin Packages for NASL and CA Certificate Upload

You can upload a custom plugin package as a .tar.gz or .tgz file. Depending on your needs, you must include a combination of the following files:

- A custom_feed_info.inc file. Always include this file to time stamp your upload to Tenable.sc Director.
- (Optional) A custom_nasl_archive.tar.gz or custom_nasl_archive.tgz file. Include this file if you are uploading one or more custom plugins.
- (Optional) A custom_CA.inc file. Include this file if you are uploading one or more CA certificates to solve a Nessus scanning issue.

After you Create the Custom Plugin Package and Upload the Custom Plugin Package, Tenable.sc Director pushes the package to Nessus for use when scanning.

**Note:** The system untars the files within your custom plugin package and overwrites any identically named files already in Tenable.sc Director or Nessus.

custom_feed_info.inc Guidelines

Always include this file to time stamp your upload to Tenable.sc Director. This text file must contain the following lines:

```plaintext
PLUGIN_SET = "YYYYMMDDHHMM";
PLUGIN_FEED = "Custom";
```

The PLUGIN_SET variable `YYYYMMDDHHMM` is the date and time 2 minutes in the future from when you plan to upload the file to Tenable.sc Director.

custom_nasl_archive.tar.gz or custom_nasl_archive.tgz Guidelines

Include this file if you are uploading one or more custom plugins. This package must contain one or more custom plugin NASL files.

All custom plugins must have unique Plugin ID numbers and have family associations based on existing Tenable.sc families.
Note: Tenable Support does not assist with creating custom plugin NASL files.

custom_CA.inc Guidelines

Include this file if you are uploading one or more CA certificates to solve a Nessus scanning issue. This text file must contain PEM-encoded (Base64) CA certificate text.

For troubleshooting information, see Troubleshooting Issues with the custom_CA.inc File.

One CA Certificate

If you need to include a single CA certificate, paste the PEM-encoded (Base64) certificate directly into the file.

```
-----BEGIN CERTIFICATE-----
certificatetext
certificatetext
certificatetext
certificatetext
certificatetext
-----END CERTIFICATE-----
```

Multiple CA Certificates

If you need to include two or more CA certificates, include the PEM-encoded (Base64) certificates back-to-back.

```
-----BEGIN CERTIFICATE-----
certificate1text
certificate1text
certificate1text
certificate1text
certificate1text
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
certificate2text
certificate2text
certificate2text
certificate2text
certificate2text
-----END CERTIFICATE-----
```
Create the Custom Plugin Package

**Required User Role:** Administrator

For complete information, see [Custom Plugin Packages for NASL and CA Certificate Upload](#).

To create the `.tar.gz` or `.tgz` custom plugin package:

1. Prepare the individual text files you want to include in the custom plugins package.
   - `custom_nasl_archive.tar.gz` or `custom_nasl_archive.tgz`
   - `custom_feed_info.inc`
   - `custom_CA.inc`

   Confirm the files meet the requirements described in [Custom Plugin Packages for NASL and CA Certificate Upload](#).

2. On the command line, tar and compress the files together. *(7-Zip or running tar on a Mac does not work for this.)* For example:

   ```
   # tar -zcvf upload_this.tar.gz custom_feed_info.inc custom_CA.inc
   ```

   The system generates a `.tar.gz` or `.tgz` file.

What to do next:

- Upload the `.tar.gz` or `.tgz` file, as described in [Upload the Custom Plugin Package](#).
Upload the Custom Plugin Package

**Required User Role:** Administrator

For complete information, see [Custom Plugin Packages for NASL and CA Certificate Upload](#).

Before you begin:

- Create the `.tar.gz` or `.tgz` custom plugin file, as described in [Create the Custom Plugin Package](#).

Upload the `.tar.gz` or `.tgz` file to Tenable.sc Director:

1. Log in to Tenable.sc Director via the user interface.

2. Click **Username > Plugins**.
   
   The **Plugins** page appears.

3. Click **Upload Custom Plugins** and select the `.tar.gz` or `.tgz` file.

4. Click **Submit**.
   
   Tenable.sc Director uploads the package and pushes it to Nessus.

What to do next:

- To verify the upload succeeded, click **System > System Logs**.

- To verify the upload resolved a validation issue, run another scan that includes plugin 51192. Verify that Nessus has the custom plugin bundle by checking its plugin directory.
Backup and Restore

Tenable recommends performing regular backups of the Tenable.sc Director data in your /opt/sc directory. When you restore a backup, the file overwrites the content in your /opt/sc directory.

Note the following limitations:

- You must restore a backup file to a Tenable.sc Director running the same version. For example, you cannot restore a backup file created on version 5.17.0 to a Tenable.sc Director running a version later than 5.17.0.

- You must restore a backup file to the same Tenable.sc Director where you created the backup file. The hostname associated with the backup file must match the hostname on the receiving Tenable.sc Director. For example, you cannot restore a backup file created on a Tenable.sc Director with the hostname Example1 to a Tenable.sc Director with the hostname Example2.

For more information, see Perform a Backup and Restore a Backup.
Perform a Backup

**Required User Role:** Root user

For more information about the backup and restore process, see [Backup and Restore](#).

To perform a backup of Tenable.sc Director data:

1. Log in to Tenable.sc Director via the user interface.

2. Stop Tenable.sc Director, as described in [Start, Stop, or Restart Tenable.sc Director](#).

   Tenable.sc Director stops.

3. Run the following command to view all running processes:

   ```bash
   # ps -fu tns
   ```

4. If any processes are listed, run the following commands to stop them:

   ```bash
   # killall -u tns
   # killall httpd
   ```

   **Note:** These commands stop all jobs (including scans) running on Tenable.sc Director.

5. If necessary, repeat step 4 to confirm all processes are stopped.

6. Run the following command to create a `.tar` file for your `/opt/sc` directory:

   ```bash
   # tar -pzcf sc_backup.tar.gz /opt/sc
   ```

   **Note:** The `.tar` file switches are case-sensitive.

   Tenable.sc Director creates the backup file.

7. Run the following command to confirm the backup file is not corrupted:
8. Move the backup file to a secure location.

9. Start Tenable.sc Director, as described in Start, Stop, or Restart Tenable.sc Director. Tenable.sc Director starts.

What to do next:

- (Optional) Restore the backup file, as described in Restore a Backup.
**Restore a Backup**

**Required User Role:** Root user

For more information about the backup and restore process, see [Backup and Restore](#).

**Before you begin:**

- Perform a backup of your Tenable.sc Director, as described in [Perform a Backup](#).
- Confirm your receiving Tenable.sc Director meets the requirements described in [Backup and Restore](#).
- Move the backup file to your receiving Tenable.sc Director's /tmp directory.

**To restore a backup file:**

1. Log in to Tenable.sc Director via the user interface.
2. Stop Tenable.sc Director, as described in [Start, Stop, or Restart Tenable.sc Director](#).
   
   Tenable.sc Director stops.
3. Run the following command to view all running processes:
   
   ```
   # ps -fu tns
   ```
4. If any processes are listed, run the following commands to stop them:
   
   ```
   # killall -u tns
   
   # killall httpd
   ```

   **Note:** These commands stop all jobs running on Tenable.sc Director.
5. If necessary, repeat step 4 to confirm all processes are stopped.
6. Run the following commands to decompress the .tar file and overwrite the existing /opt/sc directory:

```
# cd /

tar -xvf /tmp/sc_backup.tar.gz
```

**Note:** The .tar file switches are case-sensitive.

The restore finishes.

7. Start Tenable.sc Director, as described in [Start, Stop, or Restart Tenable.sc Director](#).

Tenable.sc Director starts.
Monitor Scans

See the following sections to monitor scans running on your managed Tenable.sc instances.

- Scanning Overview
- Resources
- Repositories
- Active Scan Objects
- Tags
Scanning Overview

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.

Configuring both methods provides a comprehensive view of the organization's security posture and reduces false positives. For more information about Tenable scanning strategies, see the Tenable Scan Strategy Guide.

In Tenable.sc Director, you can monitor the scans running on your managed Tenable.sc instances. Tenable.sc Director cannot run scans.

<table>
<thead>
<tr>
<th>Scan Type</th>
<th>Description</th>
<th>Licensing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery Scan</td>
<td>Find assets on your network. For example:</td>
<td>Assets identified by discovery scans do not count toward your license.</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>• an NNM instance in discovery mode.</td>
<td></td>
</tr>
<tr>
<td>Assessment Scan</td>
<td>Find vulnerabilities on your assets. For example:</td>
<td>In general, assets assessed by assessment scans count toward your license.</td>
</tr>
<tr>
<td></td>
<td>• an authenticated or unauthenticated active scan using a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nessus or Tenable.io scanner.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• an agent scan using an agent-capable Tenable.io or Nessus Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>scanner.</td>
<td></td>
</tr>
</tbody>
</table>

Authenticated Active Scans

Configure authenticated scans, also known as credentialed scans, by adding access credentials to your assessment scan configuration.

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.  

**Unauthenticated Active 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.  

For more information about how discovered and assessed assets are counted towards your license, see [License Requirements](#).
Resources

Administrator users can view supporting resources on managed Tenable.sc instances.

- **Nessus Scanners**

Scan zone resources are considered active scan objects. For more information, see [Active Scan Objects](#) and [Scan Zones](#).

LDAP server resources are part of user account configuration. For more information, see [User Accounts](#) and [LDAP Authentication](#).
Nessus Scanners

In the Tenable.sc framework, the Nessus scanner behaves as a server, while Tenable.sc serves as a client that schedules and initiates scans, retrieves results, reports results, and performs a wide variety of other important functions.

In Tenable.sc Director, you can view the Nessus scanners on your managed Tenable.sc instances.

For more information, see:

- [View Your Nessus Scanners](#)
- [View Details for a Nessus Scanner](#)

For information about Tenable.sc-Nessus communications encryption, see [Encryption Strength](#).

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A descriptive name for the scanner.</td>
</tr>
<tr>
<td>Description</td>
<td>A scanner description, location, or purpose.</td>
</tr>
<tr>
<td>Host</td>
<td>The hostname or IP address of the scanner.</td>
</tr>
<tr>
<td>Port</td>
<td>The TCP port that the scanner listens on for communications from Tenable.sc.</td>
</tr>
<tr>
<td></td>
<td>The default is port 8834.</td>
</tr>
<tr>
<td>Enabled</td>
<td>A scanner may be <strong>Enabled</strong> or <strong>Disabled</strong> within Tenable.sc to allow or prevent access to the scanner.</td>
</tr>
<tr>
<td>Verify Host-name</td>
<td>Adds a check to verify that the hostname or IP address entered in the Host option matches the CommonName (CN) presented in the SSL certificate from the Nessus server.</td>
</tr>
</tbody>
</table>

**Note:** Confirm that the correct CA certificate is configured for use by Tenable.sc. If you are using a custom CA, configure Tenable.sc to trust your custom CA, as described in [Trust a Custom CA](#). You do not need to perform this step when using the default certificates for Nessus servers.

<p>| Use Proxy | Instructs Tenable.sc to use its configured proxy for communication with the scanner. |
| Authentication Type | Select <strong>Password</strong> or <strong>SSL Certificate</strong> for the authentication type to connect to the scanner. |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Username</strong></td>
<td>Username generated during the install for daemon to client communications. This must be an administrator user in order to send plugin updates to the scanner. If the scanner is updated by a different method, such as through another Tenable.sc, a standard user account may be used to perform scans. This option is only available if the <strong>Authentication Type</strong> is set to <strong>Password</strong>.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The login password must be entered in this option. This option is only available if the <strong>Authentication Type</strong> is set to <strong>Password</strong>.</td>
</tr>
<tr>
<td><strong>Certificate</strong></td>
<td>If you set <strong>Authentication Type</strong> to <strong>SSL Certificate</strong>, specifies the nes-cert.pem file you want to use for authentication to the scanner.</td>
</tr>
<tr>
<td></td>
<td>For complete information about Nessus SSL certificate authentication, see Manual Nessus SSL Certificate Exchange.</td>
</tr>
<tr>
<td><strong>Certificate Passphrase</strong></td>
<td>If you selected <strong>SSL Certificate</strong> as the <strong>Authentication Type</strong> and the private key that decrypts your SSL certificate is encrypted with a passphrase, the passphrase for the private key.</td>
</tr>
<tr>
<td><strong>Zones</strong></td>
<td>The scan zones that can use this scanner. For more information, see Scan Zones.</td>
</tr>
<tr>
<td><strong>Agent Capable</strong></td>
<td>Specifies whether you want this scanner to provide Nessus Agent scan results to Tenable.sc.</td>
</tr>
<tr>
<td></td>
<td>Agent capable scanners must be either Tenable.io or Nessus Manager 6.5 or later. When using Nessus Manager, an organizational user account must be used to connect from Tenable.sc.</td>
</tr>
<tr>
<td><strong>Organizations</strong></td>
<td>When the <strong>Agent Capable</strong> option is enabled, specifies one or more organizations that you want to grant access to import Nessus Agent data into Tenable.sc.</td>
</tr>
<tr>
<td><strong>API Keys</strong></td>
<td>When the <strong>Agent Capable</strong> option is enabled, specifies whether you want to use secure API keys when importing agent scan data from Nessus or Tenable.io scanners.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>For more information about retrieving your access key and secret key from Nessus and Tenable.io, see <a href="#">Generate a Nessus API Key</a> in the <em>Nessus User Guide</em> and <a href="#">Generate a Tenable.io API Key</a> in the <em>Tenable.io Vulnerability Management User Guide</em>.</td>
</tr>
<tr>
<td>Access Key</td>
<td>When the <strong>API Keys</strong> option is enabled, specifies the access key for the Nessus or Tenable.io scanner.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>When the <strong>API Keys</strong> option is enabled, specifies the secret key for the Nessus or Tenable.io scanner.</td>
</tr>
</tbody>
</table>
# Nessus Scanner Statuses

You can view the status for scanners, as described in [View Your Nessus Scanners](#).

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Error</td>
<td>Tenable.sc could not authenticate to the scanner using the credentials you provided.</td>
<td>Check your <a href="#">scanner configuration settings</a> and confirm the <strong>Username</strong> and <strong>Password</strong> options specify valid login credentials for the scanner.</td>
</tr>
<tr>
<td>Certificate Mismatch</td>
<td>Tenable.sc could not confirm the validity of the SSL certificate presented by the scanner.</td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <a href="#">Edit your scanner configuration</a> and select a different authentication type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- (Nessus scanners only) Check your <a href="#">scanner configuration settings</a> and confirm the <strong>Certificate</strong> option specifies the correct nessuscert.pem file. For more information about managing SSL certificates in Nessus, see <a href="#">Manage SSL Certificates</a> in the <a href="#">Nessus User Guide</a>.</td>
</tr>
<tr>
<td>Connection Error</td>
<td>Tenable.sc cannot connect to the scanner because the scanner is unreachable or does not exist at the IP address or hostname provided.</td>
<td>Do one or both of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <a href="#">Check your scanner configuration</a> and confirm the <strong>Host</strong> option specifies the correct IP address or hostname for the scanner.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Confirm the network devices and firewalls between Tenable.sc and the scanner are configured to permit network traffic.</td>
</tr>
<tr>
<td>Connection Timeout</td>
<td>Tenable.sc connected to the scanner but timed out waiting for a reply.</td>
<td>Contact your network administrator for troubleshooting assistance.</td>
</tr>
<tr>
<td>Invalid Configuration</td>
<td>The scanner attempted to connect to a scanner on</td>
<td><a href="#">Check your scanner configuration</a> and confirm the <strong>Port</strong> option specifies a valid TCP port to con-</td>
</tr>
</tbody>
</table>

---

Copyright © 2020 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>Port 0.</th>
<th>nect to your scanners. For more information, see Port Requirements.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugins Out of Sync</td>
<td>The plugin sets on the scanner do not match the plugin sets in Tenable.sc.</td>
</tr>
<tr>
<td>Protocol Error</td>
<td>Tenable.sc connected to the scanner but the scanner returned an HTTPS protocol negotiation error.</td>
</tr>
<tr>
<td>Reloading Scanner</td>
<td>The scanner is temporarily unable to run scans because Nessus is restarting on the scanner.</td>
</tr>
<tr>
<td>Requires Upgrade</td>
<td>The version of Nessus on the scanner is end-of-life.</td>
</tr>
<tr>
<td>Updating Plugins</td>
<td>Tenable.sc is performing a plugin update on the scanner.</td>
</tr>
<tr>
<td>Updating Status</td>
<td>Tenable.sc is refreshing the status of the scanner. Scanners can continue to run scans while Tenable.sc refreshes the status.</td>
</tr>
</tbody>
</table>

**Note:** Tenable.sc automatically refreshes scanner statuses every 15 minutes.
<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Disabled</td>
<td>A Tenable.sc user disabled the scanner.</td>
<td>Edit your scanner configuration and click the Enabled toggle to re-enable the scanner. For more information about scanner options, see Nessus Scanners.</td>
</tr>
<tr>
<td>Working</td>
<td>The scanner is connected to Tenable.sc and able to run scans.</td>
<td>None.</td>
</tr>
</tbody>
</table>
Manage Nessus Scanners

**Required User Role:** Administrator

For more information, see [Nessus Scanners](#).

To manage your Nessus scanners:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Scan Infrastructure > Scanners**.
   
   The **Nessus Scanners** page appears.
3. To filter the scanners that appear on the page, apply a filter as described in [Apply a Filter](#).
4. To view the list of configured scanners, see [View Your Nessus Scanners](#).
5. To view details for a scanner, see [View Details for a Nessus Scanner](#).
View Your Nessus Scanners

**Required User Role:** Administrator

For more information, see [Nessus Scanners](#).

To view a list of configured Nessus scanners:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Scan Infrastructure > Nessus Scanners.**
   The **Nessus Scanners** page appears.
3. View details about each Nessus scanner.
   - **Name** — The name for the scanner.
   - **Tenable.sc Instance** — The name of the Tenable.sc instance where the scanner is configured. For more information, see [Managing Tenable.sc Instances with Tenable.sc Director](#).
   - **Features** — Specifies whether the scanner is a **Standard** scanner or an **Agent Capable** scanner. Agent capable scanners provide Nessus Agent scan results to Tenable.sc.
   - **Status** — The status of the scanner. For more information, see [Nessus Scanner Statuses](#).
   - **Host** — The IP address or hostname of the scanner.
   - **Version** — The scanner's Nessus version.
   - **Type** — The type of scanner connection.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td>Tenable.sc could not identify the scanner.</td>
</tr>
<tr>
<td>Nessus (Unmanaged Plugins)</td>
<td>Tenable.sc accesses the scanner using a Nessus user account with <strong>Standard</strong> permissions. Tenable.sc cannot send plugin updates to the scanner or manage the scanner's activation code.</td>
</tr>
<tr>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Nessus (Managed Plugins)</td>
<td>Tenable.sc manages the scanner and authenticates via a Nessus user account. Tenable.sc sends plugin updates to the scanner and manages the scanner's activation code.</td>
</tr>
<tr>
<td>Tenable.io (Unmanaged Plugins)</td>
<td>Tenable.sc.accesses the instance using a Tenable.io user account with <strong>Standard</strong> permissions. Tenable.sc cannot send plugin updates to the instance or manage the instance's activation code.</td>
</tr>
</tbody>
</table>

- **Uptime** — The length of time, in days, that the scanner has been running.
- **Last Modified** — The date and time the scanner was last modified.

4. To view details of a specific Nessus scanner, see **View Details for a Nessus Scanner**.
5. To filter the scanners that appear on the page, apply a filter as described in **Apply a Filter**.
6. To manually refresh the **Status** data, in the **Options** drop-down box, click **Update Status**.

Tenable.sc Director refreshes the **Status** data.
# View Details for a Nessus Scanner

**Required User Role:** Administrator

For more information, see [Nessus Scanners](#).

To view details for a Nessus scanner:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Scan Infrastructure > Nessus Scanners**.
   
   The **Nessus Scanners** page appears.

3. In the row for the scanner for which you want to view details, click the menu.
   
   The actions menu appears.

4. Click **View**.

   The **View Nessus Scanner** page appears.

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
</table>
| **Options** drop-down box | • To edit the scanner, click **Edit**.  
  • To delete the scanner, click **Delete**, as described in Delete a Nessus Scanner.  
  • To download logs for the scanner, click **Download Logs**. For more information, see Download Nessus Scanner Logs. |
| **General** | View general information about the scanner. |
| **Authentication** | View authentication information for the scanner. |
| **Active Scans** | View active scan information for the scanner. |
| **Agents** | View agent information for the scanner.  
  • **Agent Capable** — Specifies whether the scanner is agent capable: **Yes** or **No**. |
<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organizations</strong></td>
<td>If the scanner is agent capable, the organization configured for the scanner.</td>
</tr>
<tr>
<td><strong>API Keys Set</strong></td>
<td>If the scanner is agent capable, specifies whether API keys are configured for the scanner: Yes or No.</td>
</tr>
</tbody>
</table>

**Data summary**

View metadata and performance metrics for the scanner.

**Note:** Tenable.sc Director refreshes the load information every 15 minutes.

**Nessus Scanner Health**

If you are viewing details for a managed Nessus scanner running version 8.2.0 or later, view scanner health summary data:

- **Running Scans** — The number of scans currently running on the scanner.
- **Hosts Being Scanned** — The number of hosts currently being scanned by the scanner.
- **CPU Load** — The percent of the total CPU currently in use by the scanner.
- **Total Memory** — The total memory installed on the scanner.
- **Memory Used** — The percent of the total memory currently in use by the scanner.
- **Total Disk Space** — The total disk space installed on the scanner.
- **Disk Space Used** — The percent of the total disk space currently in use by the scanner.
- **Last Updated** — The date and time Tenable.sc last updated the scanner data.

Tenable.sc refreshes the data when you load the View Nessus Scanner page. To force a manual refresh, click the button.
Start, Pause, or Stop Scans on a Managed Tenable.sc Instance

**Required User Role:** Tenable.sc Director Administrator

From Tenable.sc Director, you can pause, resume, and stop scans that are running on managed Tenable.sc instances.

- If you pause a scan, the scan temporarily stops scanning targets. You can resume a paused scan at any time.
- If you stop a scan, you can choose to create a rollover scan.

For more information about connecting managed Tenable.sc instances to Tenable.sc Director, see [Managing Tenable.sc Instances with Tenable.sc Director](#).

To pause, resume, or stop scans on a managed Tenable.sc instance:

1. Log in to Tenable.sc Director via the user interface.

2. Click **Scan Results**.
   
The **Scan Results** page appears.

3. To pause a running scan:
   
   - In the row for the scan you want to pause, click the **Pause** button.
   
   Tenable.sc pauses the scan on the managed Tenable.sc instance.

4. To resume a paused scan:
   
   - In the row for the scan you want to resume, click the **Resume** button.
   
   Tenable.sc resumes the paused scan on the managed Tenable.sc instance.

5. To stop a running scan:
   
   a. In the row for the scan you want to stop, click the **Actions** menu.
   
   The actions menu appears.

   b. Click **Stop**.

   c. Click one of the following options to determine how the managed Tenable.sc instance handles the results of the stopped scan:

---

Copyright © 2020 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.
- **Discard Results** — The managed Tenable.sc instance does not import any of the results obtained by the scan to the database.

- **Import Results** — The managed Tenable.sc instance imports the results of the current scan and discards the information for the unscanned hosts.

- **Import Results and Create Rollover** — The managed Tenable.sc instance imports the results from the scan into the database and creates a rollover scan that you can launch manually to complete the scan.

Tenable.sc stops the scan on the managed Tenable.sc instance.
Repositories

Repositories are databases within Tenable.sc Director that contain vulnerability data. You can share repositories with users and organizations based on admin-defined assets. Repositories provide scalable and configurable data storage. Optionally, you can share repository data between multiple Tenable.sc deployments.

**Note:** The maximum repository size is 32 GB.

When adding an external repository, you access a local repository from another Tenable.sc. Remote repositories allow you to share repository data from one Tenable.sc deployment to your primary Tenable.sc deployment via an SSH session.

External repository data is static and used solely for reporting purposes. For more information, see [External Repositories](#).

For more information, see [Add a Repository](#) and [Manage Repositories](#). For information about Tenable.sc Director repository data encryption, see [Encryption Strength](#).

**Tip:** If you need to remove data from a repository (for example, to remove retired asset data or to resolve a license issue), see the [knowledge base](#) article.
Manage Repositories

**Required User Role:** Administrator

For more information, see [Repositories](#).

To manage your repositories:

1. Log in to Tenable.sc Director via the user interface.

2. Click [Repositories](#).
   
   The [Repositories](#) page appears.

3. To filter the repositories that appear on the page, apply a filter as described in [Apply a Filter](#).

4. To view details for a repository:
   
   a. In the row for the repository, click the menu.
      
      The actions menu appears.

   b. Click [View](#).
      
      The [View Repository](#) page appears. For more information, see [Repository Details](#).

5. To edit a repository:
   
   a. In the row for the repository, click the menu.
      
      The actions menu appears.

   b. Click [Edit](#).
      
      The [Edit Repository](#) page appears.

   c. Modify the repository options, as described in [Remote Repositories](#).

   d. Click [Submit](#).
      
      Tenable.sc Director saves your configuration.

6. To export a repository, see [Export a Repository](#).
View Repository Details

**Required User Role:** Administrator

You can view details for any repository. For more information, see [Repositories](#).

To view repository details:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Repositories > Repositories**.
   The **Repositories** page appears.
3. In the row for the repository, click the menu.
   The actions menu appears.
4. Click **View**.
   The **View Repository** page appears.

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>View general information for the repository.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong> — The repository name.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Description</strong> — The repository description.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Created</strong> — The date the repository was created.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Last Modified</strong> — The date the repository was last modified.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ID</strong> — The repository ID.</td>
</tr>
<tr>
<td>Data</td>
<td>View a summary of the repository data (for example, the IP address range). For more information, see <a href="#">Remote Repositories</a>.</td>
</tr>
<tr>
<td>Access</td>
<td>View the name of the organizations with access to this repository.</td>
</tr>
<tr>
<td>Advanced Settings</td>
<td>View a summary of your settings for the repository. For more information about a setting, see <a href="#">Remote Repositories</a>.</td>
</tr>
</tbody>
</table>
Export a Repository

**Required User Role:** Administrator

You can export a repository from one Tenable.sc and import it as an offline repository on another Tenable.sc. For more information, see Offline Repositories.

**Note:** Depending on the size of the repository database, this file can be quite large. It is important to save the file to a location with sufficient free disk space.

To export a repository:

1. Log in to Tenable.sc Director via the user interface.

2. Click **Repositories > Repositories**.

   The **Repositories** page appears.

3. In the row for the repository, click the **menu**.

   The actions menu appears.

4. Click **Export**.

   Tenable.sc Director exports the repository.

What to do next:

- To import the repository to another Tenable.sc, add an offline repository to that Tenable.sc as described in **Add a Repository**.
External Repositories

When adding an external repository, you access a local repository from another Tenable.sc:

- Offline repositories allow you to share repository data from one Tenable.sc deployment to your primary Tenable.sc deployment via manual export and import (a .tar.gz archive file). You can combine data from several repository files into a single offline repository by importing multiple files to the offline repository.

- Remote repositories allow you to share repository data from one Tenable.sc deployment to your primary Tenable.sc deployment via an SSH session.

External repository data is static and used solely for reporting purposes. For more information, see Offline Repositories and Remote Repositories.

For more information, see Repositories and Add a Repository.
Remote Repositories

Remote repositories allow you to share repository data from one Tenable.sc deployment to your primary Tenable.sc deployment via an SSH session.

**Note:** You must upgrade both Tenable.sc deployments to version 5.7.1 or later in order to configure agent repositories as remote repositories.

**Note:** You cannot set a remote repository as the Import Repository for active scans. You can use remote repository data only for reporting purposes.

For more information, see Add a Repository.

To use tiered remote repositories for large enterprise deployments of Tenable.sc, see Tiered Remote Repositories.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The repository name.</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive text for the repository.</td>
</tr>
<tr>
<td>Remote Tenable.sc</td>
<td></td>
</tr>
<tr>
<td>Host</td>
<td>The IP address for the host you want to synchronize with to obtain repository data. After you type the IP address:</td>
</tr>
<tr>
<td></td>
<td>1. Click <strong>Request Repositories</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Type the username and password for an administrator account on the remote Tenable.sc.</td>
</tr>
<tr>
<td></td>
<td>The Tenable.sc deployments exchange SSH keys, and the system populates the Repository list with all available repositories from the remote Tenable.sc.</td>
</tr>
<tr>
<td>Repository</td>
<td>The remote repository you want to collect IP addresses and vulnerability data from.</td>
</tr>
<tr>
<td>Update Schedule</td>
<td>Sets the schedule for the remote server to be queried for updated information.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Access</td>
<td>Specifies which organizations have access to the vulnerability data stored in the repository. If groups are configured for the organization, Tenable.sc prompts you to grant or deny access to all of the groups in the organization. For more granular control, grant access within the settings for that group.</td>
</tr>
</tbody>
</table>
# Active Scan Objects

Complete Tenable.sc scan configurations rely on the following scan objects. For information about active scans, see Active Scans.

<table>
<thead>
<tr>
<th>Scan Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>assets</td>
<td>Assets are lists of devices (e.g., laptops, servers, tablets, phones, etc.) within a Tenable.sc organization. Assets can be shared with one or more users based on local security policy requirements. You can add an asset to group devices that share common attributes. Then, you can use the asset during scan configuration to target the devices in the asset. For more information, see <a href="#">Assets</a>.</td>
</tr>
<tr>
<td>credentials</td>
<td>Credentials are reusable objects that facilitate a login to a scan target. Various types of credentials with different authentication methods can be configured for use within scan policies. Credentials may be shared between users for scanning purposes. Tenable.sc supports an unlimited number of SSH, Windows, and database credentials, and four SNMP credential sets per scan configuration. For more information, see <a href="#">Credentials</a>.</td>
</tr>
<tr>
<td>audit files</td>
<td>During a configuration audit, auditors verify that servers and devices are configured according to an established standard and maintained with an appropriate procedure. Tenable.sc can perform configuration audits on key assets through the use of Nessus' local checks that can log directly onto a Unix or Windows server without an agent. Tenable.sc supports a variety of audit standards. Some of these come from best practice centers like the PCI Security Standards Council and the Center for Internet Security (CIS). Some of these are based on Tenable's interpretation of audit requirements to comply with specific industry standards such as PCI DSS or legislation such as Sarbanes-Oxley. In addition to base audits, it is easy to create customized audits for the particular requirements of any organization. These customized audits can be loaded into the Tenable.sc and made available to anyone performing configuration audits within an organization.</td>
</tr>
</tbody>
</table>
NIST SCAP files can be uploaded and used in the same manner as an audit file. Navigate to NIST's SCAP website ([http://scap.nist.gov](http://scap.nist.gov)) and under the SCAP Content section, download the desired SCAP security checklist zip file. The file may then be uploaded to Tenable.sc and selected for use in Nessus scan jobs.

Once the audit scan policies are configured in Tenable.sc, they can be repeatedly used. Tenable.sc can also perform audits intended for specific assets. Through the use of audit policies and asset lists, a Tenable.sc user can quickly determine the compliance posture for any specified asset.

For more information, see [Audit Files](#).

### scan zones

Scan zones represent areas of your network that you want to target in an active scan, associating an IP address or range of IP addresses with one or more scanners in your deployment. Scan zones define the IP address ranges associated with the scanner along with organizational access.

For more information, see [Scan Zones](#).

### scan policies

Scan policies contain options related to performing an active scan. For example:

- Options that control technical aspects of the scan such as timeouts, number of hosts, type of port scanner, and more.
- Options that provide plugin family-based or individual plugin-based scan specifications.
- Options that control compliance policy checks (Windows, Linux, Database, etc.), report verbosity, service detection scan settings, audit files, patch management systems, and more.

For more information, see [Scan Policies](#).
Assets

Tenable.sc Director assets are lists of devices (e.g., laptops, servers, tablets, phones, etc.) within a Tenable.sc Director organization. Assets can be shared with one or more users based on local security policy requirements.

You can add an asset to group devices that share common attributes. Then, you can use the asset during scan configuration to target the devices in the asset. Examples of common attributes include:

- IP address ranges
- hardware types
- vulnerabilities
- outdated software versions
- operating systems

Tenable.sc Director supports template-based and custom assets. For more information, see Add an Asset from a Template and Add a Custom Asset. To view details for any of your assets, see View Asset Details.

Template-based Assets

Tenable provides asset templates that you can customize for your environment. Tenable-provided asset templates are updated via the Tenable.sc feed and visible depending on other configurations.

Custom Assets

Tenable.sc Director supports the following custom assets types: Static Assets, DNS Name List Assets, LDAP Query Assets, Combination Assets, Dynamic Assets, Watchlist Assets, and Import Assets.

Static Assets

Static assets are lists of IP addresses. You can use static assets immediately after configuration.

For example, if your organization assigns laptops within a defined IP address range, you can create a custom static asset for laptops using that IP address range.
Option | Description
---|---
Name | A name for the asset.
Description | A description for the asset.
Tag | A tag for the asset. For more information, see Tags.
IP Addresses | IP addresses to include within the asset (20,000 character limit).
| Type a comma-delimited list of IP addresses, CIDR addresses, or ranges.
| Upload a .txt file containing a comma-delimited list of IP addresses, CIDR addresses, or ranges.

DNS Name List Assets

Option | Description
---|---
Name | A name for the asset.
Description | A description for the asset.
DNS Names | The DNS hostnames for the asset to be based upon.

LDAP Query Assets

The LDAP Query asset type appears if an LDAP server is configured within your organization.

Option | Description
---|---
Name | A name for the asset.
Description | A description for the asset.
LDAP Server | The LDAP server where you want to perform the query.

**Note:** If the LDAP server is configured to use a different DNS server than Tenable.sc Director, Tenable.sc Director cannot resolve hostnames retrieved from the LDAP server.

**Note:** Tenable.sc Director cannot retrieve more than one page of LDAP results. If Tenable.sc Director asset or user authentication queries are not retrieving all expected results,
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the asset.</td>
</tr>
<tr>
<td>Description</td>
<td>A description for the asset.</td>
</tr>
<tr>
<td>Combination</td>
<td>This option accepts multiple existing assets utilizing the operators AND, OR, and NOT. Using these operators and multiple existing assets, new unique assets may be created. If the source assets change, the Combination asset updates to match the new conditions. When this option is initially selected, the options of <strong>NOT</strong> and a list of existing assets are displayed. Selecting one of those options followed by a space will display the next valid option for building the asset and continue until the selections are complete. If the border for the combination option is red it is an indication that there is a problem in the logic of the query.</td>
</tr>
</tbody>
</table>

**Combination Assets**

Combination assets allow you to create an asset based on existing assets and the AND, OR, and NOT operators.

Combination assets can include agent IDs if the asset contains exclusively dynamic assets. You may experience unexpected asset behavior if your combination asset contains other asset types and interacts with agent repository data.

**Dynamic Assets**
Dynamic assets are flexible groups of condition statements that Tenable.sc Director uses to retrieve a list of devices meeting the conditions. Tenable.sc Director refreshes dynamic asset lists using the results from Tenable.sc scans. You cannot use dynamic assets until after Tenable.sc performs an initial discovery scan and retrieves a list of devices.

Dynamic assets can include agent IDs.

For example, in the asset above, Tenable.sc Director retrieves a list of Linux systems listening on TCP Port 80. For more information about constructing dynamic asset conditions, see Dynamic Assets.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the asset.</td>
</tr>
<tr>
<td>Description</td>
<td>A description for the asset.</td>
</tr>
<tr>
<td>Asset Definition</td>
<td>Defines the rules for creating a dynamic asset list. Hovering over an existing rule will give the ability to add, edit, or delete a group or a rule to the definition.</td>
</tr>
</tbody>
</table>

Dynamic Asset Rule Logic
<table>
<thead>
<tr>
<th>Valid Operators</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Plugin ID</strong></td>
<td></td>
</tr>
<tr>
<td>is equal to</td>
<td>Value must be equal to value specified.</td>
</tr>
<tr>
<td>not equal to</td>
<td>Value must be not equal to value specified.</td>
</tr>
<tr>
<td>is less than</td>
<td>Value must be less than the value specified.</td>
</tr>
<tr>
<td>is greater than</td>
<td>Value must be greater than the value specified.</td>
</tr>
<tr>
<td><strong>Plugin Text</strong></td>
<td></td>
</tr>
<tr>
<td>is equal to</td>
<td>Value must be equal to value specified.</td>
</tr>
<tr>
<td>not equal to</td>
<td>Value must be not equal to value specified.</td>
</tr>
<tr>
<td>contains the pat-</td>
<td>Value must contain the text specified (e.g., ABCDEF contains ABC).</td>
</tr>
<tr>
<td>tern</td>
<td></td>
</tr>
<tr>
<td>Posix regex</td>
<td>Any valid Posix regex pattern contained within “/” and “/” (example: /.<em>ABC.</em>)</td>
</tr>
<tr>
<td>Perl compatible</td>
<td>Any valid Perl compatible regex pattern.</td>
</tr>
<tr>
<td>regex</td>
<td></td>
</tr>
<tr>
<td><strong>Operating System</strong></td>
<td></td>
</tr>
<tr>
<td>is equal to</td>
<td>Value must be equal to value specified.</td>
</tr>
<tr>
<td>not equal to</td>
<td>Value must be not equal to value specified.</td>
</tr>
<tr>
<td>contains the pat-</td>
<td>Value must contain the text specified (e.g., ABCDEF contains ABC).</td>
</tr>
<tr>
<td>tern</td>
<td></td>
</tr>
<tr>
<td>Posix regex</td>
<td>Any valid Posix regex pattern contained within “/” and “/” (e.g., /.<em>ABC.</em>)</td>
</tr>
<tr>
<td>Perl compatible</td>
<td>Any valid Perl compatible regex pattern.</td>
</tr>
<tr>
<td>regex</td>
<td></td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td></td>
</tr>
<tr>
<td>is equal to</td>
<td>Value must be equal to value specified.</td>
</tr>
<tr>
<td>not equal to</td>
<td>Value must be not equal to value specified.</td>
</tr>
<tr>
<td><strong>DNS, NetBIOS Host, NetBIOS Workgroup, MAC, SSH v1 Fingerprint, SSH v2 Fingerprint</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Valid Operators</strong></td>
<td><strong>Effect</strong></td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>is equal to</td>
<td>Value must be equal to value specified.</td>
</tr>
<tr>
<td>not equal to</td>
<td>Value must be not equal to value specified.</td>
</tr>
<tr>
<td>contains the pattern</td>
<td>Value must contain the text specified (e.g., 1.2.3.124 contains 124).</td>
</tr>
<tr>
<td>Posix regex</td>
<td>Any valid Posix regex pattern contained within “/” and “/” (e.g., /.<em>ABC.</em>)</td>
</tr>
<tr>
<td>Perl compatible regex</td>
<td>Any valid Perl compatible regex pattern.</td>
</tr>
</tbody>
</table>

**Port, TCP Port, UDP Port**

<table>
<thead>
<tr>
<th><strong>is equal to</strong></th>
<th><strong>Value must be equal to value specified.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>not equal to</strong></td>
<td><strong>Value must be not equal to value specified.</strong></td>
</tr>
<tr>
<td><strong>is less than</strong></td>
<td><strong>Value is less than value specified.</strong></td>
</tr>
<tr>
<td><strong>is greater than</strong></td>
<td><strong>Value is greater than the value specified.</strong></td>
</tr>
</tbody>
</table>

**Days Since Discovery, Days Since Observation**

<table>
<thead>
<tr>
<th><strong>is equal to</strong></th>
<th><strong>Value must be equal to value specified. Scroll arrows are provided to allow for entry selection or the value can be manually entered. Max 365.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>not equal to</strong></td>
<td><strong>Value must be not equal to value specified. Scroll arrows are provided to allow for entry selection or the value can be manually entered. Max 365.</strong></td>
</tr>
<tr>
<td><strong>is less than</strong></td>
<td><strong>Value is less than value specified. Scroll arrows are provided to allow for entry selection or the value can be manually entered. Max 365.</strong></td>
</tr>
<tr>
<td><strong>is greater than</strong></td>
<td><strong>Value is greater than the value specified. Scroll arrows are provided to allow for entry selection or the value can be manually entered. Max 365.</strong></td>
</tr>
<tr>
<td><strong>where Plugin ID is</strong></td>
<td><strong>Any valid Plugin ID number. Multiple Plugin IDs may be entered using a range and/or comma separated Plugin IDs (e.g., 3, 10189, 34598, 50000-55000, 800001-800055).</strong></td>
</tr>
</tbody>
</table>

**Severity**

<table>
<thead>
<tr>
<th><strong>is equal to</strong></th>
<th><strong>Value must be equal to value specified (info, low, medium, high, or critical).</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>not equal to</strong></td>
<td><strong>Value must be not equal to value specified (info, low, medium, high, or crit-</strong></td>
</tr>
</tbody>
</table>
Valid Operators | Effect
---|---
| ical). |
is less than | Value must be less than the value specified (info, low, medium, high, or critical).
is greater than | Value must be greater than the value specified (info, low, medium, high, or critical).
where Plugin ID is | Any valid Plugin ID number. Multiple Plugin IDs may be entered using a range and/or comma separated Plugin IDs (e.g., 3, 10189, 34598, 50000-55000, 800001-800055).

Exploit Available

| Is | Click **True** or **False** in the drop-down box.

Exploit Frameworks

| is equal to | Value must be equal to value specified.
is not equal to | Value must not be equal to value specified.
contains the pattern | Value must contain the pattern entered.

XRef

| Value must be in the XRef option.

Watchlist Assets

A watchlist is an asset that is used to maintain lists of IPs not in the user’s managed range of IP addresses. IPs from a watchlist can be filtered on regardless of your IP address range configuration. This proves to be beneficial when analyzing event activity originating outside of the user’s managed range. For example, if a block of IP addresses is a known source of malicious activity, it could be added to a Malicious IPs watchlist and added to a custom query.

**Note:** Watchlists only uses event data to create the asset list.

| Option | Description |
---|---|
Name | A name for the asset. |
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A description for the asset.</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>IP addresses to include within the asset list (20,000 character limit). One address, CIDR address, or range can be entered per line. Click <strong>Choose File</strong> to import a list of IP addresses from a saved file.</td>
</tr>
</tbody>
</table>

### Import Assets

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The asset name.</td>
</tr>
<tr>
<td>Asset</td>
<td>Click <strong>Choose File</strong> to choose the asset that was previously exported for import into Tenable.sc Director.</td>
</tr>
</tbody>
</table>
**Add an Asset from a Template**

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

To add an asset from a Tenable-provided template:

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **Assets**.
   
   The **Assets** page appears.
3. Click **Add**.
   
   The **Add Assets** page appears.
4. (Optional) If you want to search for a specific asset template, type a search phrase in the **Search Templates** box.
5. In the **Templates** section, click a template type.
   
   The **Add Asset Template** page for the template type appears.
6. View the available templates. In each row:
   
   - the four square icon (墀) on the left side indicates a collection of several assets.
   - the data icons (墀, LCE, N) on the right side indicate the data required to build the asset.
   
   The NNM (PVS), LCE, and NS icons indicate you must have NNM, LCE, or Nessus data. The key icon (キー) indicates you must have credentials for the device. The notepad icon (ノート) indicates you must have compliance data.
7. (Optional) If you want to search for a specific asset template, type a search phrase in the **Search Templates** box or select a category from the **All** drop-down box.
8. Click the row for the template you want to use.
   
   The detail page for the template type appears.
9. Click **Add**.
   
   The **Assets** page appears.
10. Click the row for the asset you just added.

   The **Edit** page appears.

11. View the details for the asset.

12. (Optional) If necessary, edit the asset to customize it for your environment. For more information about asset options, see [Assets](#).

13. Click **Submit**.

   Tenable.sc Director saves your configuration.
Add a Custom Asset

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

To add a custom asset:

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **Assets**.
   
   The **Assets** page appears.
3. Click **Add**.
   
   The **Add Assets** page appears.
4. In the **Custom** section, click an asset type.
   
   The **Add Assets** page for the asset type appears.
5. Configure the required options for the asset type, as described in **Assets**.
6. Click **Submit**.
   
   Tenable.sc Director saves your configuration.
**View Asset Details**

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

You can view details for any asset. For more information, see [Assets](#).

To view asset details:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Assets**.
   
The **Assets** page appears.
3. In the row for the asset, click the ⚙ menu.
   
The actions menu appears.
4. Click **View**.
   
The **View Asset** page appears.

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>View general information for the asset.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong> — The asset name.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Description</strong> — The asset description.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Tag</strong> — The tag applied to the asset. For more information, see <a href="#">Tags</a>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Addresses</strong> (static assets only) — The IP addresses specified in the asset. For more information, see <a href="#">Assets</a>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Created</strong> — The date the asset was created.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Last Modified</strong> — The date the asset was last modified.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Owner</strong> — The username for the user who created the asset.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Group</strong> — The group in which the asset belongs.</td>
</tr>
<tr>
<td>Section</td>
<td>Action</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Tenable.io Synchronization Data</td>
<td>View synchronization summary data:</td>
</tr>
<tr>
<td></td>
<td>• <strong>ID</strong> — The asset ID.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Status</strong> — The status of the asset in Lumin synchronization:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Finished</strong> — The most recent synchronization that included this asset succeeded.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Not Synced</strong> — The asset is not configured for Lumin synchronization.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Error</strong> — An error occurred. For more information, see View Lumin Data Logs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>First Synchronization</strong> — The date and time of the first synchronization of this asset.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Last Success</strong> — The date and time of the most recent synchronization of this asset.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Last Failure</strong> — The date and time of the most recent failed synchronization of this asset.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Details</strong> — If the <strong>Status</strong> is <strong>Error</strong>, details about the error.</td>
</tr>
<tr>
<td></td>
<td>For more information about Lumin synchronization, see Lumin Synchronization.</td>
</tr>
</tbody>
</table>
Audit Files

The Nessus vulnerability scanner allows you to perform compliance audits of numerous platforms including (but not limited to) databases, Cisco, Unix, and Windows configurations as well as sensitive data discovery based on regex contained in audit files. Audit files are XML-based text files that contain the specific configuration, file permission, and access control tests to be performed. For more information, see Manage Audit Files.

After you create an audit file, you can reference the audit file in a template-based Policy Compliance Auditing scan policy or a custom scan policy. For more information about compliance options in custom scan policies, see Compliance Options.

Template-Based Audit Files

You can add template-based audit files using templates embedded within Tenable.sc Director. Tenable updates these templates regularly through the Tenable.sc feed.

For more information, see Add a Template-Based Audit File.

Custom Audit Files

You can add custom audit files to upload any of the following:

- a Tenable-created audit file downloaded from the Tenable downloads page.
- a Security Content Automation Protocol (SCAP) Data Stream file downloaded from a SCAP repository (e.g., https://nvd.nist.gov/ncp/repository).
  
  The file must contain full SCAP content (Open Vulnerability and Assessment Language (OVAL) and Extensible Configuration Checklist Description Format (XCCDF) content) or OVAL standalone content.

  **Note:** XCCDF standalone content audit files lack automated checks and do not return scan results in Tenable.sc.

- a custom audit file created or customized for a specific environment. For more information, see the knowledge base article.

For more information, see Add a Custom Audit File.
Add a Template-Based Audit File

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

You can add template-based audit files using templates embedded within Tenable.sc Director. Tenable updates these templates regularly through the Tenable.sc feed.

For more information, see [Audit Files](#).

To add a template-based audit file:

1. Log in to Tenable.sc.
2. Click **Audit Files**.
   - The Audit Files page appears.
3. Click **Add**
   - The Add Audit File page appears.
4. In the **Templates** section, click a template category tile.
   - The Add Audit Template page appears.
5. In the **Name** box, type a name for the audit file.
6. (Optional) In the **Description** box, type a description for the audit file.
7. (Optional) Edit the template-specific options if you do not want to use the default values.
8. Click **Submit**.
   - Tenable.sc Director saves your configuration.

What to do next:

- Reference the audit file in a template-based Policy Compliance Auditing scan policy or a custom scan policy. For more information about compliance options in custom scan policies, see [Compliance Options](#).
Add a Custom Audit File

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

You can add custom audit files to upload any of the following:

- a Tenable-created audit file downloaded from the [Tenable downloads](#) page.
- a Security Content Automation Protocol (SCAP) Data Stream file downloaded from a SCAP repository (e.g., [https://nvd.nist.gov/ncp/repository](https://nvd.nist.gov/ncp/repository)).

The file must contain full SCAP content (Open Vulnerability and Assessment Language (OVAL) and Extensible Configuration Checklist Description Format (XCCDF) content) or OVAL standalone content.

**Note:** XCCDF standalone content audit files lack automated checks and do not return scan results in Tenable.sc.

- a custom audit file created or customized for a specific environment. For more information, see the [knowledge base](#) article.

For more information, see [Audit Files](#).

**Before you begin:**

- Download or prepare the file you intend to upload.

**To add a custom audit file or SCAP Data Stream file:**

1. Log in to Tenable.sc via the user interface.
2. Click **Audit Files**.

   The **Audit Files** page appears.
3. Click **Add**

   The **Add Audit File** page appears.
4. In the **Custom** section, click the **Advanced** tile.
5. In the **Name** box, type a descriptive name for the audit file.
6. In the **Description** box, type a description for the audit file.

7. Click **Choose File** and browse to the **Audit File** you want to upload.

   The system uploads the file. If you uploaded a SCAP Data Stream file, additional options appear.

8. If you uploaded a Data Stream file with full SCAP content, continue configuring options for the file:

   a. If you uploaded SCAP 1.2 content or later, in the **Data Stream Name** box, select the Data Stream identifier found in the SCAP 1.2 Data Stream content.

   b. In the **Benchmark Type** box, select the operating system that the SCAP content targets.

   c. In the **Benchmark Name** box, select the benchmark identifier found in the SCAP XCCDF component.

   d. In the **Profile** box, select the benchmark profile identifier found in the SCAP XCCDF component.

   e. (Optional) If you want to define benchmark tailoring separately from the SCAP XCCDF benchmark, click **Choose File** and browse to the **Tailoring File** you want to upload.

      The system uploads the file.

9. Click **Submit**.

   Tenable.sc Director saves your configuration.

What to do next:

- Reference the audit file in a template-based Policy Compliance Auditing scan policy or a custom scan policy. For more information about compliance options in custom scan policies, see Compliance Options.
Manage Audit Files

**Required User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Audit Files.

To manage your audit files:

1. Log in to Tenable.sc Director via the user interface.
2. Click Audit Files.
   
   The Audit Files page appears.
3. To filter the audit files that appear on the page, apply a filter as described in Apply a Filter.
4. To add an audit file, see Add a Template-Based Audit File or Add a Custom Audit File.

5. To view details for an audit file:
   a. In the row for the audit file, click the menu.
   b. Click View.
      
      The View Audit File page appears.

6. To edit or replace an audit file:
   a. In the row for the audit file, click the menu.
   b. Click Edit.
   c. To edit the name or description, type a new Name or Description.
   d. To replace the audit file, click the delete button next to the file and upload a new audit file.
   e. Click Submit.
      
      Tenable.sc Director saves your configuration.

7. To share or revoke access to an audit file:
   (This is the Drop-down text)
a. In the row for the audit file, click the menu.

b. Click Share.

c. Share or revoke access for each group in your organization.

d. Click Submit.

Tenable.sc Director saves your configuration.

8. To export an audit file:

a. In the row for the audit file, click the menu.

b. Click Export.

Tenable.sc Director exports the audit file.

9. To delete an audit file:

a. In the row for the audit file, click the menu.

b. Click Delete.

A confirmation window appears.

c. Click Delete.

Tenable.sc Director deletes the audit file.
Scan Zones

Scan zones are areas of your network that you want to target in an active scan, associating an IP address or range of IP addresses with one or more scanners in your deployment. You must create scan zones in order to run active scans in your managed Tenable.sc instances.

In Tenable.sc Director, you can monitor scan zones on your managed Tenable.sc instances.

For more information, see View Your Scan Zones.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the scan zone.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) A description for the scan zone.</td>
</tr>
<tr>
<td>Ranges</td>
<td>One or more IP addresses that you want the scan zone to target. Supported formats:</td>
</tr>
<tr>
<td></td>
<td>• a comma-separated list of IP addresses and/or CIDR addresses.</td>
</tr>
<tr>
<td></td>
<td>• a newline-separated list of IP addresses and/or CIDR addresses.</td>
</tr>
<tr>
<td></td>
<td>• a hyphenated range of IP addresses (e.g., 192.0.2.0-192.0.2.25).</td>
</tr>
<tr>
<td>Scanners</td>
<td>One or more scanners that you want to use to scan the Ranges in this scan zone.</td>
</tr>
</tbody>
</table>

**Note:** Do not choose scanners that cannot reach the areas of your network identified in the Ranges. Similarly, consider the quality of the network connection between the scanners you choose and the Ranges.
View Your Scan Zones

**Required User Role:** Administrator

For more information, see [Scan Zones](#).

To view a list of configured scan zones:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Scan Infrastructure > Scan Zones**.
   
   The **Scan Zones** page appears.

3. View details about each scan zone.
   
   - **Name** — The name for the scan zone.
   
   - **Tenable.sc Instance** — The name of the Tenable.sc instance where your scan zone is configured. For more information, see [Managing Tenable.sc Instances with Tenable.sc Director](#).
   
   - **Status** — The status of the scan zone.

<table>
<thead>
<tr>
<th>Scan Zone Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Scanners Available</td>
<td>All of the scanners in the scan zone are <strong>Working</strong>.</td>
</tr>
<tr>
<td>x/y Scanners Available</td>
<td>Only some of the scanners in the scan zone are <strong>Working</strong>.</td>
</tr>
<tr>
<td>No Scanners Available</td>
<td>None of the scanners in the scan zone are <strong>Working</strong>.</td>
</tr>
</tbody>
</table>

For information about **Working** and other scanner statuses, see [Nessus Scanner Statuses](#).

- **Scanners** — The number of Nessus scanners in the scan zone.

- **Last Modified** — The date and time the scan zone was last modified.
Tags

You can use tags in Tenable.sc Director to label assets or queries with a custom descriptor to improve filtering and object management. For example, you could add a tag named **East Coast Employees** to label all of your assets in that geographic area.

After you create a tag and apply it to an object, the tag is visible to all users who can view or modify that object. However, tags are not shared across object types.

For more information, see [Add a Tag](#) and [Remove or Delete a Tag](#).
Add a Tag

**Required User Role:** Tenable.sc Director organizational user with appropriate permissions. For more information, see [User Roles](#).

For more information, see [Tags](#).

To add a tag:

1. Log in to Tenable.sc Director.
2. Navigate to the assets or queries page:
   - Click [Assets](#).
   - Click [Analysis > Queries](#).
3. In the row for the asset or query you want to tag, click the menu. The actions menu appears.
4. Click [Edit](#).
5. In the [Tag](#) drop-box, select an existing tag or type a new tag.
6. Click [Submit](#).
   
   The tag appears, applied to the asset or query.
Remove or Delete a Tag

**Required User Role:** Tenable.sc Director organizational user with appropriate permissions. For more information, see User Roles.

You can remove a tag from an asset or query to stop associating that object with the tag. To completely delete a tag from Tenable.sc Director, you must remove the tag from all assets or queries. For more information, see Tags.

To remove a tag or completely delete a tag from Tenable.sc Director:

1. Log in to Tenable.sc Director via the user interface.
2. Navigate to the assets or queries page:
   - Click Assets.
   - Click Analysis > Queries.
3. In the row for the asset or query where you want to remove the tag, click the menu.
   The actions menu appears.
4. Click Edit.
5. In the Tag drop-box, remove the tag from the asset or query.
6. Click Submit.
   Tenable.sc Director removes the tag from the asset or query.
7. (Optional) If you want to delete the tag from Tenable.sc Director, repeat steps 2 through 6 until you have removed all uses of the tag for the object type.
   Tenable.sc Director deletes the tag.
## Analyze Data

See the following sections to analyze and respond to Tenable.sc Director data.

<table>
<thead>
<tr>
<th>Analysis Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Results</td>
<td>View a table of scan results from active and agent scans.</td>
</tr>
<tr>
<td>Dashboards</td>
<td>View graphical summaries of scans, scan results, and system activity.</td>
</tr>
<tr>
<td>Solutions Analysis</td>
<td>View recommended solutions for all vulnerabilities on your network.</td>
</tr>
<tr>
<td>Vulnerability Analysis</td>
<td>View a table of cumulative or mitigated vulnerability data.</td>
</tr>
<tr>
<td>Reports</td>
<td>Create custom or template-based reports to export Tenable.sc data for further analysis.</td>
</tr>
</tbody>
</table>

You can use Filters and Queries to manipulate the data you see in analysis tools and save views for later access. You can perform Workflow Actions (alerting and ticketing) from some analysis tools.
Dashboards

**Required User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

Administrator users can view Tenable-provided Insights dashboard. For more information, see Insights Dashboard.

Organizational users can configure custom or template-based dashboards that contain dashboard components, which display vulnerability, event, ticket, user, and alert data for analysis. When viewing vulnerability or event data, you can drill into the underlying data set for further evaluation.

**Tip:** Tenable provides many dashboard templates (e.g., the VPR Summary dashboard). For a complete index of Tenable-provided dashboard templates, see the Tenable.sc Dashboards blog.

Dashboards allow you to organize similar dashboard components to streamline your analysis. Instead of creating a single dashboard with several dozen dashboard components, you can create several dashboards that group similar dashboard components together. For example, you can create two separate dashboards to view active scanning data and passive scanning data.

**Note:** Dashboards display vulnerability, event, and other scan data. Tenable recommends configuring several data sources to optimize the data you see in dashboards. For more information, see Scanning Overview.

For more information, see:

- View a Dashboard
- Add a Template-Based Dashboard
- Add a Custom Dashboard
- Import a Dashboard
- Manage Dashboards
- Manage Dashboard Components
View a Dashboard

**Required User Role:** Administrator or organizational user with appropriate permissions. For more information, see [User Roles](#).

For more information, see [Dashboards](#).

To view a dashboard:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Dashboard**.
   
The **Dashboards** page appears, displaying your default dashboard.
3. If you want to switch to a different dashboard:
   
a. In the upper-right corner of the page, click the **Switch Dashboard** drop-down box.
   
   b. Click the dashboard you want to view.
   
   The dashboard appears.

   If you are an organizational user, you can:

   - Add a dashboard component to the dashboard in view, as described in [Add a Template-Based Dashboard Component](#) or [Add a Custom Dashboard Component](#).

   - Manage dashboard components on the dashboard in view, as described in [Manage Dashboard Components](#).

   - Edit the dashboard settings for the dashboard in view, as described in [Edit Settings for a Dashboard](#).

   - Share or revoke access to the dashboard in view, as described in [Share or Revoke Access to a Dashboard](#).

   - Create a report from the dashboard in view:

     a. In the upper-right corner of the page, click the **Options** drop-down box.

     b. Click **Send to Report**.

     For more information about reports, see [Reports](#).
• Delete the dashboard in view, as described in Delete a Dashboard.
## Insights Dashboard

Tenable.sc Director provides the **Insights** dashboard to administrators. For more information, see [View a Dashboard](#).

<table>
<thead>
<tr>
<th>Widget</th>
<th>Action</th>
</tr>
</thead>
</table>
| Scanners Connection Status | • View the total number of scanners on all managed Tenable.sc instances and the percentage of scanners that are **Working** or **Not Working**. For information about **Working** and other scanner statuses, see [Nessus Scanner Statuses](#).  
  • To view the list of all **Working** scanners, click the green section of the circle graph.  
  • To view the list of all **Not Working** scanners, click the red section of the circle graph.  
  
  **Note:** **Not Working** includes all scanner statuses other than **Working**. For more information about all possible scanner statuses, see [Nessus Scanner Statuses](#). |
| Scan Zones Status          | • View the total number of scan zones on all managed Tenable.sc instances and the percentage of scan zones that are **Working**, **Degraded**, or **Not Working**. For information about **Working** and other scan zone statuses, see [View Your Scan Zones](#).  
  • To navigate to a list of all **Working** scan zones, click the green section of the circle graph.  
  • To navigate to a list of all **Degraded** scan zones, click the orange section of the circle graph.  
  • To navigate to a list of all **Not Working** scan zones, click the red section of the circle graph. |
| Tenable.sc Instance Status | View the total number of managed Tenable.sc instances and the percentage of scan zones that are **Connected** or experiencing a **Connection Error**.                                                                 |

---

Copyright © 2020 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>Widget</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugin Set Age</td>
<td>View the elapsed time since the last plugin update on your managed Tenable.sc instances, by plugin age:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Within 24 Hours</strong> — The number of instances with plugins updated within the last 24 hours.</td>
</tr>
<tr>
<td></td>
<td>• <strong>1-7 Days Old</strong> — The number of instances with plugins updated between 1 day and 7 days ago.</td>
</tr>
<tr>
<td></td>
<td>• <strong>8-14 Days Old</strong> — The number of instances with plugins updated between 8 days and 14 days ago.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Older Than 14 Days</strong> — The number of instances with plugins updated more than 14 days ago.</td>
</tr>
<tr>
<td>Scan Results Trend</td>
<td>View the status of scan results on your managed Tenable.sc instances, by date, within the selected time frame (last 24 hours, last 7 days, or last 30 days). For more information about scan result statuses, see <strong>Scan Result Statuses</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Completed</strong> — The number of scans that completed successfully.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Partial</strong> — The number of scans that ran, but did not complete.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Failed</strong> — The number of scans that failed to run.</td>
</tr>
<tr>
<td></td>
<td>To change the time frame of the scan results shown, click the selectors above the graph:</td>
</tr>
<tr>
<td></td>
<td>• <strong>24H</strong> — View scan result statuses from the last 24 hours.</td>
</tr>
<tr>
<td></td>
<td>• <strong>7D</strong> — View scan result statuses from the last 7 days.</td>
</tr>
<tr>
<td></td>
<td>• <strong>30D</strong> — View scan result statuses from the last 30 days.</td>
</tr>
<tr>
<td></td>
<td>To show or hide a status in the graph, click the name of the status in the key below the graph.</td>
</tr>
<tr>
<td></td>
<td>To navigate to a list of <strong>Completed</strong> scan results, click the green section of the graph.</td>
</tr>
<tr>
<td>Widget</td>
<td>Action</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• To navigate to a list of <strong>Partial</strong> scan results, click the orange section of the graph.</td>
</tr>
<tr>
<td></td>
<td>• To navigate to a list of <strong>Failed</strong> scan results, click the red section of the graph.</td>
</tr>
<tr>
<td>Scanning Overview</td>
<td>• View a list of all scans that are <strong>Running</strong> or <strong>Paused</strong> on your managed Tenable.sc instances, by Tenable.sc instance name and scan name. Scans with a purple bar are <strong>Running</strong> and scans with a grey bar are <strong>Paused</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Hover over the timeline for a scan to view additional details:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Tenable.sc Instance</strong> — The name of the managed Tenable.sc instance where the scan is running.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Progress</strong> — The number of scanned hosts compared to the total number of hosts to scan.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Started</strong> — The date and time the scan started.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Estimated Time</strong> — The estimated time to scan completion.</td>
</tr>
</tbody>
</table>
Set a Dashboard as Your Default Dashboard

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

For more information, see [Dashboards](#).

To set a dashboard as your default dashboard:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Dashboard > Dashboard**.
   
   The **Dashboards** page appears, displaying your default dashboard.
3. If you want to switch to a different dashboard:
   a. In the upper-right corner of the page, click the **Switch Dashboard** drop-down box.
   b. Click the dashboard you want to view.
   
   The dashboard appears.
4. In the upper-right corner of the page, click the **Options** drop-down box.
5. Click **Set as Default**.
   
   The system sets the dashboard as your default.
Share or Revoke Access to a Dashboard

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

You can share access to a dashboard to give users in a group the ability to view the dashboard. The user's role and custom permissions determine if they can drill down into other pages with more information. For more information, see [Dashboards](#).

To share or revoke access to a dashboard:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Dashboard > Dashboard**.
   
   The **Dashboards** page appears, displaying your default dashboard.
3. If you want to switch to a different dashboard:
   a. In the upper-right corner of the page, click the **Switch Dashboard** drop-down box.
   b. Click the dashboard you want to view.
   
   The dashboard appears.
4. In the upper-right corner of the page, click the **Options** drop-down box.
5. Click **Share**.
   
   The **Share Dashboard** window appears.
6. In the box, search for and select the groups for which you want to share or revoke access.
7. Click **Submit**.
   
   Tenable.sc Director saves your configuration.
Delete a Dashboard

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

For more information, see [Dashboards](#).

To delete a dashboard:

1. Log in to Tenable.sc via the user interface.
2. Click **Dashboard > Dashboard**.
   
   The **Dashboards** page appears, displaying your default dashboard.
3. If you want to switch to a different dashboard:
   a. In the upper-right corner of the page, click the **Switch Dashboard** drop-down box.
   b. Click the dashboard you want to view.
      
      The dashboard appears.
4. In the upper-right corner of the page, click the **Options** drop-down box.
5. Click **Delete**.
   
   A confirmation window appears.
6. Click **Delete**.
   
   The system deletes the dashboard.
Add a Template-Based Dashboard

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

For more information, see [Dashboards](#).

To add a template-based dashboard:

1. Log in to Tenable.sc via the user interface.

2. Click **Dashboard > Dashboard**.

   The **Dashboards** page appears.

3. In the upper-right corner of the page, click the **Options** drop-down button.

4. Click **Add Dashboard**

   The **Add Dashboard** page appears.

5. In the **Templates** section, click a template category tile.

   The **Add Dashboard Template** page appears.

6. Click a template.

   The **Add Dashboard Template** page updates to reflect the template you selected.

7. Modify the dashboard template:

   - To edit the dashboard name, click the name box and edit the name.
   - To edit the dashboard description, click the **Description** box and edit the description.
   - To restrict the target data displayed in the dashboard, click the **Targets** drop-down box.

8. Click **Add**.

   Tenable.sc saves your configuration and the **Dashboards** page appears.

9. In the upper-right corner of the page, click the **Switch Dashboard** drop-down box.

10. Click the name of the dashboard you just created.

    The page for the dashboard appears.
What to do next:

- Add dashboard components, as described in Add a Template-Based Dashboard Component or Add a Custom Dashboard Component.
Add a Custom Dashboard

**Required User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Dashboards.

To add a custom dashboard:

1. Log in to Tenable.sc via the user interface.
2. Click Dashboard > Dashboard.
   
The Dashboards page appears.
3. In the upper-right corner of the page, click the Options drop-down button.
4. Click Add Dashboard
   
The Add Dashboard page appears.
5. In the Custom section, click the Advanced tile.
6. In the Name box, type a name for the dashboard.
7. In the Description box, type a description for the dashboard.
8. In the Layout section, select the layout you want to use for the dashboard.
9. Click Submit.
   
Tenable.sc saves your configuration and the Dashboards page appears.
10. In the upper-right corner of the page, click the Switch Dashboard drop-down box.
11. Click the name of the dashboard you just created.
   
The page for the dashboard appears.

What to do next:

- Add dashboard components, as described in Add a Template-Based Dashboard Component or Add a Custom Dashboard Component.
Import a Dashboard

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

For more information, see [Dashboards](#).

To import a dashboard:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Dashboard**.
   
   The **Dashboards** page appears.
3. In the upper-right corner of the page, click the **Options** drop-down button.
4. Click **Add Dashboard**.
   
   The **Add Dashboard** page appears.
5. In the **Custom** section, click the **Import** tile.
   
   The **Import Dashboard** page appears.
6. In the **Name** box, type a name for the dashboard.
7. Click the **Choose File** button and browse to the dashboard file you want to import.
8. Click **Submit**.
   
   Tenable.sc Director imports the dashboard.
Manage Dashboards

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

For more information, see [Dashboards](#).

To manage dashboards:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Dashboard**.
   
   The **Dashboards** page appears.
3. In the upper-right corner of the page, click the **Options** drop-down button.
4. Click **Manage Dashboards**.
   
   The **Manage Dashboards** page appears.
5. To add a dashboard, click **Add**. For more information, see [Add a Template-Based Dashboard](#) or [Add a Custom Dashboard](#).
6. To filter the dashboards in the table, see [Apply a Filter](#).
7. To manage a single dashboard, click the ⚙ menu in a dashboard row.
   
   The actions menu appears.
   
   From this menu, you can:

   - Click **View** to view details for the dashboard.
   - Click **Edit** to edit the dashboard. For more information, see .
   - Click **Share** to share or revoke access to the dashboard.
   - Click **Copy** to copy the dashboard.
   - Click **Delete** to delete the dashboard.
8. To show or hide a dashboard from the **Switch Dashboard** drop-down on the **Dashboards** page, pin or unpin the dashboard:
- pinned, the dashboard appears.
- unpinned, the dashboard does not appear.

To export the dashboard as an XML file:

a. Click Export.

b. Then, identify how you want Tenable.sc to handle object references:

   ○ **Remove All References** – all object references are removed, altering the definitions of the components. Importing users do not need to make any changes for components to be useable.

   ○ **Keep All References** – object references are kept intact. Importing users must be in the same organization and have access to all relevant objects for the components to be useable.

   ○ **Replace With Placeholders** – object references are removed and replaced with their respective names. Importing users see the name of the reference object, but need to replace it with an applicable object within their organization before the component is useable.

**Note:** Due to version-specific changes in dashboard XML file formats, exported dashboards are not always compatible for import between Tenable.sc Director versions.
Manage Dashboard Components

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

For more information, see [Dashboards](#).

To manage dashboard components:

1. Log in to Tenable.sc Director via the user interface.
2. Click [Dashboard](#).
   
   The [Dashboards](#) page appears.

To edit a dashboard component:

1. Hover over the dashboard component.
2. Click the menu.
   
   The actions menu appears.
3. Click [Edit](#).

To view the data behind a dashboard component:

1. Hover over the dashboard component.
2. Click the arrow icon.
   
   The analysis page appears.

**Note:** Only dashboard components that display vulnerability analysis or event analysis data support viewing the data behind a dashboard component.

To reorder a dashboard component:

1. Click the title of a dashboard component.
2. Drag the dashboard component around the page.
To copy a dashboard component to the dashboard in view or a different dashboard:

1. Hover over the dashboard component.
2. Click the menu.
   - The actions menu appears.
3. Click **Copy**.
4. In the **Name** box, edit the name for the copied dashboard component.
5. In the **Dashboard** drop-down box, click the name of the dashboard where you want to copy the dashboard component.
6. Click **Copy**.
   - Tenable.sc Director copies the dashboard component.

To refresh the dashboard component data:

1. Hover over the dashboard component.
2. Click the menu.
   - The actions menu appears.
3. Click **Refresh**.
   - Tenable.sc Director refreshes the dashboard component data.

To delete the dashboard component:

1. Hover over the dashboard component.
2. Click the menu.
   - The actions menu appears.
3. Click **Delete**.
   - A confirmation window appears.
4. Click **Delete**.
   - Tenable.sc Director deletes the dashboard component.
Add a Template-Based Dashboard Component

**Required User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Dashboards.

Before you begin:

- Add a dashboard, as described in Add a Template-Based Dashboard, Add a Custom Dashboard, or Import a Dashboard.

To add a template-based dashboard component to a dashboard:

1. Log in to Tenable.sc via the user interface.
2. Click Dashboard.
   The Dashboards page appears.
3. In the upper-right corner of the page, click the Switch Dashboard drop-down box.
4. Click the name of the dashboard for which you want to add a component.
   The dashboard appears.
5. In the upper-right corner of the page, click the Options drop-down box.
6. Click Add Component.
   The Add Component page appears.
7. Click the template you want to use for the dashboard component.
   The Add Component Template page updates to reflect the template you selected.
8. Modify the dashboard component template:

   - To edit the dashboard component name, click the name box and edit the name.
   - To edit the dashboard component description, click the Description box and edit the description.
• To restrict the target data displayed in the dashboard component, click the **Targets** dropdown box.

9. Click **Add**.

Tenable.sc saves your configuration and the **Dashboards** page appears.
Add a Custom Dashboard Component

Required User Role: Organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Dashboards.

Before you begin:

- Add a dashboard, as described in Add a Template-Based Dashboard, Add a Custom Dashboard, or Import a Dashboard.

To add a custom dashboard component to a dashboard:

1. Log in to Tenable.sc via the user interface.
2. Click Dashboard.
   
The Dashboards page appears.
3. In the upper-right corner of the page, click the Switch Dashboard drop-down box.
4. Click the name of the dashboard for which you want to add a component.
   
The page for the dashboard appears.
5. In the upper-right corner of the page, click the Options drop-down box.
6. Click Add Component.
   
The Add Component page appears.
7. In the Custom section, click the type of component you want to configure.
   
The Add Table Component page, Add Bar Chart Component page, Add Pie Chart Component page, Add Matrix Component page, Add Line Chart Component page, or Add Area Chart Component page appears.
8. Configure the options for your component type, as described in Custom Dashboard Component Options.
9. Click Submit.
   
   Tenable.sc Director saves your configuration.

Copyright © 2020 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.
Custom Dashboard Component Options

First, configure general options for your component.

<table>
<thead>
<tr>
<th>General Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the dashboard component.</td>
</tr>
<tr>
<td>Description</td>
<td>A description for the dashboard component. The <strong>Description</strong> appears on the Dashboards page when you hover over a dashboard component.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Frequency with which the component polls the data source to obtain updates. Available frequency options include: minutely (15 minutes, 20 minutes, 30 minutes), hourly (1 hours, 2 hours, 4 hours, 6 hours, 12 hours), daily (default) with a time of day, weekly repeating every 1-20 weeks and selection of the day(s) of week, monthly repeating every 1-20 months (by day or date), and never. <strong>Caution:</strong> Excessively frequent updates may cause the application to become less responsive due to the added processing load imposed on the host OS.</td>
</tr>
</tbody>
</table>

Then, configure specific options for your component type: [Table Component Options](#), [Bar Chart Component Options](#), [Pie Chart Component Options](#), [Line and Area Chart Component Options](#) or [Matrix Component Options](#).

Table Component Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td></td>
</tr>
<tr>
<td>Query</td>
<td>Predefined query used to further narrow down the data source options. If a query does not exist or is not desired, it may be left unselected. The query may be used as is or as a template on which to base the Filters option.</td>
</tr>
<tr>
<td>Type</td>
<td>Vulnerability, Mobile, Event, Ticket, Alert, or User.</td>
</tr>
<tr>
<td>Source</td>
<td>For vulnerability data type, sources include <strong>Cumulative</strong> or <strong>Mitigated</strong> depending on the desired data source. For event type, the source defaults to <strong>Active</strong>.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Note:</strong> <strong>Source</strong> option is not available because only active event data is permitted for event-based components.</td>
<td></td>
</tr>
<tr>
<td>Tool</td>
<td>Determines the analysis tool to use for creating the chart.</td>
</tr>
<tr>
<td>Filters</td>
<td>Additional filters to use on the data source. For more information, see <strong>Filters</strong>.</td>
</tr>
<tr>
<td><strong>Display</strong></td>
<td></td>
</tr>
<tr>
<td>Results Displayed</td>
<td>The number of displayed results (maximum: 999). If the <strong>Viewport Size</strong> setting is smaller than this setting, the results display is limited to the <strong>Viewport Size</strong> setting with a scrollbar to display the additional results.</td>
</tr>
<tr>
<td>Viewport Size</td>
<td>The number of records (maximum: 50) to display along with a scrollbar to handle additional records. For example, if <strong>Results Displayed</strong> is set to <strong>100</strong> and <strong>Viewport Size</strong> is <strong>15</strong>, 15 records are displayed with a scrollbar to view the additional 85 records.</td>
</tr>
<tr>
<td>Sort Column</td>
<td>(Except Event Data Type) Column that the results are sorted by.</td>
</tr>
<tr>
<td>Sort Direction</td>
<td>(Except Event Data Type) <strong>Descending</strong> (default) or <strong>Ascending</strong>.</td>
</tr>
<tr>
<td>Display Columns</td>
<td>Desired columns to be shown in the component output.</td>
</tr>
</tbody>
</table>

**Bar Chart Component Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data</strong></td>
<td></td>
</tr>
<tr>
<td>Query</td>
<td>Predefined query used to further narrow down the data source options. If a query does not exist or is not desired, it may be left unselected. The query may be used as is or as a template on which to base the Filters option.</td>
</tr>
<tr>
<td>Type</td>
<td>Vulnerability, Mobile, Event, Alert, or Ticket.</td>
</tr>
<tr>
<td>Source</td>
<td>For vulnerability data type sources, include <strong>Cumulative</strong> or <strong>Mitigated</strong> depending on the desired data source. For event type, the source defaults to <strong>Active</strong>.</td>
</tr>
</tbody>
</table>
# Pie Chart Component Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data</strong></td>
<td></td>
</tr>
<tr>
<td>Query</td>
<td>Predefined query used to further narrow down the data source options. If a query does not exist or is not desired, it may be left unselected. The query may be used as is or as a template on which to base the Filters option.</td>
</tr>
<tr>
<td>Type</td>
<td>Vulnerability, Mobile, Event, or Ticket</td>
</tr>
<tr>
<td>Source</td>
<td>For vulnerability data type sources If <strong>Data Type</strong> of <strong>Vulnerability</strong> is chosen, sources include: <strong>Cumulative</strong> or <strong>Mitigated</strong> depending on the desired data source. For event type, the source defaults to <strong>Active</strong>.</td>
</tr>
</tbody>
</table>

**Note:** The **Source** option is not available because only active event data is permitted for event-based components.
### Option | Description
--- | ---
**Tool** | Determines the analysis tool to use for creating the chart.
**Filters** | Vulnerability, Event, or Ticket filters used to narrow down the series source. For more information, see [Filters](#).

### Display

**Results Displayed** | The number of displayed results (default: 10).
**Sort Column** | Column that the results are sorted by.
**Sort Direction** | **Descending** (default) or **Ascending**.
**Display Columns** | Desired columns shown in the component output.

### Line and Area Chart Component Options

### Option | Description
--- | ---
**Data** | **Date Type** | The date type can be relative to the current time when the chart is loaded or an absolute time frame that is the same on each page visit.
**Date Range** | Available options include:
  - Last Minutes – 15, 20, 30
  - Last Hours – 1, 2, 4, 6, 12, 24 (default), 48, 72
  - Last Days – 5, 7, 25, 50
  - Last Months – 3, 6, 12
**Add/Edit Series**
**Name** | Series name
**Data** |
### Option | Description
--- | ---
**Data Type** | Note: For line/area charts, vulnerability data analysis often requires that the underlying repository be a trending repository. If the selected repository is not a trending repository, no historical analysis is available.

**Vulnerability or Event.**

**Query** | Predefined query used to further narrow down the data source options. If a query does not exist or is not desired, it may be left unselected. The query may be used as is or as a template on which to base the Filters option.

**Filters** | Filters used to narrow down the series source. For more information, see Filters.

**Display** | 

**Series Data** | Data to display in the chart (Total, Info, Low, Medium, High, Critical).

---

### Matrix Component Options

For information about configuring matrix components and to download samples, visit the [Tenable.sc Dashboards blog](https://www.tenable.com/dashboards).

### Option | Description
--- | ---
**Cells** | 

**Size** | Creating a Matrix chart starts with defining the size. Tenable.sc supports matrices from 1x1 to 10x10. Click the Generate Cells link to create the initial blank matrix which may be populated and further defined with settings described below.

**Column (max 10)** | Columns are normally used to define a group of vulnerability, mobile, event, ticket, user, or alert data. For example, five columns could be used in a matrix component, one each for critical, high, medium, low, and informational vulnerabilities. Hover the cursor over the right-hand side of the top cell of a column to display a drop-down box.

The header drop-down box contains three options: Edit Header, Delete Cells, and Copy.

Click on the Edit Header option to set the column name and update frequency. The update frequency determines how often the underlying data set is refreshed. Refresh-
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Row (max 10)</td>
<td>Rows are another grouping element, used to define the operations being performed against each column element for that row. For example, if each column determines the vulnerability type (critical, high, medium, low, and informational), a row could be created labeled <strong>Ratio</strong>. Each cell in that row could be used to calculate the ratio of the particular vulnerability type count against the total vulnerability count.</td>
</tr>
<tr>
<td></td>
<td>Hover the cursor over the right-hand side of the cell in a row entry to display a drop-down box. The box contains options to <strong>Edit Header</strong>, <strong>Delete Cells</strong>, and <strong>Copy</strong>.</td>
</tr>
<tr>
<td></td>
<td>Click on <strong>Edit Header</strong> to change the header name for the row.</td>
</tr>
<tr>
<td></td>
<td>Click on <strong>Delete Cells</strong> to delete the row of cells. There is not a confirmation window.</td>
</tr>
<tr>
<td></td>
<td>Click on <strong>Copy</strong> to copy the current row, which may then be edited as needed. Once 10 rows exist, the <strong>Copy</strong> option is no longer available.</td>
</tr>
<tr>
<td>Editing Cells</td>
<td>Cells contain the actual data operations. Cells are defined by query and condition options. Click on a cell to modify the cell definition. The options are described below:</td>
</tr>
<tr>
<td>Query Options</td>
<td>For more information, see <a href="#">Matrix Component Query Options</a>.</td>
</tr>
<tr>
<td>Display Options</td>
<td>The display options determine the background and foreground colors along with any custom text, if applicable.</td>
</tr>
</tbody>
</table>

**Rules**
There are two basic types of rules in a matrix cell definition: the default (or fallback) rule and rule(s) that are added. By default, a single editable rule is added to each cell definition. This rule cannot be deleted and describes what appears in the cell if no other conditions have been defined or triggered. A default condition looks similar to the following:

![Rules](image1)

This rule can be edited to display any of the available display options. Added rules may look similar to the following:

![Rules](image2)

When hovered over, a rule displays an edit and a delete icon. To save edits to a rule, click the checkmark icon or click the x icon to cancel the changes.

Rules are reviewed from top to bottom and trigger the display rule on the first rule match. Once a rule triggers, none of the subsequent rules are reviewed. If none of the added rules match, the default rule is automatically performed.

Matrix Component Query Options
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Type</td>
<td>Available types include: <strong>Query Value, Static Text, Icon, Bar, and Ratio</strong></td>
</tr>
<tr>
<td>Data Type</td>
<td>Available data types include <strong>vulnerability, mobile, event, ticket, alert, and user</strong>. The query value rules displayed in the condition section are dynamically defined by the data type used. For example, if a data type of <strong>Event</strong> is chosen, query value rules include <strong>Event Count, IP Count, or Port Count.</strong></td>
</tr>
<tr>
<td>Filters</td>
<td>Filter the data based on specific parameters.</td>
</tr>
<tr>
<td>Rules Type</td>
<td>Available types include: <strong>Query Value, Static Text, Icon, Bar, and Ratio.</strong></td>
</tr>
<tr>
<td>Rule</td>
<td><strong>Note:</strong> <strong>Bar and Ratio</strong> charts use ratios rather than counts in the lists below.</td>
</tr>
</tbody>
</table>

- **Vulnerability:** IP Count, Port Count, Score Count, and Vulnerability Count
- **Mobile:** Vulnerability Count, Device Count, and Score Count
- **Event:** IP Count, Port Count, Score Count, and Event Count
- **Ticket:** Ticket Count
- **Alert:** Alert Count
- **User:** User Count
Configure a Simple Matrix Dashboard Component

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

Before you begin:

- Begin adding a custom matrix dashboard component, as described in [Add a Custom Dashboard Component](#).

To construct a simple matrix dashboard component:

1. On the Add Matrix Component page, in the **Name** box, type a name for the dashboard component.
2. Type a **Description** for the dashboard component.
3. In the **Cells** section, select the number of **Columns** and **Rows** for the matrix.
For example, 5 columns and 3 rows.

4. Click **Generate Cells**.

   The matrix editor appears.

5. Next to the header label, click the ☰ menu.

   The actions menu appears.

6. Click **Edit Header**.

7. Type a **Label** for the column or row header.

8. Click **Submit**.

   The matrix editor appears, with the new header label displayed.

9. Repeat the header label steps for the other header cells.

10. Hover over the body cells and click the edit icon.

    The **Add Matrix Component** page appears.

11. Customize the matrix component options.

    For example, this matrix component displays Vulnerability data by a ratio from the Cumulative database. The numerator filters are looking for vulnerabilities that have an exploit available with
a Critical severity and were discovered within the last 7 days. The Denominator filters are for vulnerabilities that have a Critical severity and were discovered within the last 7 days. The rules are looking for percentages of the vulnerabilities that match and designate the ratio value with the corresponding color based on the percentages found.

12. Repeat the body cell steps for the other body cells.

In the example above, the other cells are similar with many of the same rules. The differences are adding a Numerator filter to include the Exploit Framework we are looking for and a Denominator filter for the Exploit Available option.
13. Click **Submit**.

   The matrix element appears.
Scan Results

The **Scan Results** page displays scan results and statuses from scans running on your managed Tenable.sc instances.

For more information, see [Manage Scan Results](#) and [Scan Result Statuses](#).
Scan Result Statuses

You can view the scan status and the import status for scans running on your managed Tenable.sc instances, as described in View Scan Result Details.

- **Scan Status**
- **Import Status**
- **Availability**

Scan Status

The scan status specifies the status of the scan.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Scans</td>
<td></td>
</tr>
<tr>
<td>Queued</td>
<td>The scan is queued.</td>
</tr>
<tr>
<td>Preparing</td>
<td>Tenable.sc is preparing to run the scan.</td>
</tr>
<tr>
<td>Resolving Hostnames</td>
<td>Tenable.sc is resolving hostnames before running the scan.</td>
</tr>
<tr>
<td>Verifying Targets</td>
<td>Tenable.sc is verifying targets before running the scan.</td>
</tr>
<tr>
<td>Initializing Scanners</td>
<td>Tenable.sc is initializing scanners before running the scan.</td>
</tr>
<tr>
<td>Running</td>
<td>The scan is running.</td>
</tr>
<tr>
<td>Pausing</td>
<td>You paused the scan and Tenable.sc is pausing the scan.</td>
</tr>
<tr>
<td>Paused</td>
<td>The scan is paused.</td>
</tr>
<tr>
<td>Resuming</td>
<td>You resumed the scan and Tenable.sc is resuming the scan.</td>
</tr>
<tr>
<td>Stopping</td>
<td>Tenable.sc is stopping the scan.</td>
</tr>
<tr>
<td>Completed</td>
<td>The scan finished successfully.</td>
</tr>
<tr>
<td>Partial</td>
<td>The scan finished and some results are available.</td>
</tr>
<tr>
<td>Error</td>
<td>The scan did not finish.</td>
</tr>
</tbody>
</table>

Agent Scans
<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queued</td>
<td>The scan is queued.</td>
</tr>
<tr>
<td>Running</td>
<td>The scan is running.</td>
</tr>
<tr>
<td>Completed</td>
<td>The scan finished successfully.</td>
</tr>
<tr>
<td>Error</td>
<td>The scan did not finish.</td>
</tr>
</tbody>
</table>

**Import Status**

The scan status specifies the status of the scan result import to Tenable.sc.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active and Agent Scans</td>
<td></td>
</tr>
<tr>
<td>No Results</td>
<td>The scan finished successfully but yielded no results.</td>
</tr>
<tr>
<td>Pending</td>
<td>Tenable.sc is preparing to start the import.</td>
</tr>
<tr>
<td>Importing</td>
<td>Tenable.sc is importing the scan result data.</td>
</tr>
<tr>
<td>Finished</td>
<td>The import finished successfully.</td>
</tr>
<tr>
<td>Error</td>
<td>The import did not finish.</td>
</tr>
</tbody>
</table>

**Availability**

The scan result availability specifies whether the scan result can be viewed in Tenable.sc Director.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>Tenable.sc Director successfully imported the scan result data.</td>
</tr>
</tbody>
</table>

**Note:** By default, Tenable.sc Director retains scan results from managed Tenable.sc instances for 30 days. For more information, see Data Expiration Settings.
<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synced</td>
<td>If the scan status is <strong>Partial</strong> or <strong>Completed</strong>, you can manually retrieve the scan result. For more information, see <a href="#">Manage Scan Results</a>.</td>
</tr>
</tbody>
</table>
Manage Scan Results

**Required User Role:** Administrator or organizational user with appropriate permissions. For more information, see [User Roles](#).

Depending on the state of a scan result, you can perform different management actions (e.g., you cannot download results for a scan with errors).

For more information, see [Scan Results](#).

To manage scan results:

1. Log in to Tenable.sc via the user interface.
2. Click **Scan Results** (administrator users) or **Scans > Scan Results** (organizational users).

   The **Scan Results** page appears.

3. Manage the results:

   To filter the scan results:
   
   - Click the filter icon.

   Filters allow you to view only desired scan results. Filter parameters include the **Name**, **Group**, **Owner**, **Scan Policy**, **Status**, **Completion Time**, **Access**, and **Type**.

   To remove all filters:
   
   - Under the filter options, click **Clear Filters**.

   **Note:** To return to the default filter for your user account, refresh your browser window. The number in grey next to the filter displays how many filters are currently in use.

   To view a set of scan results:
   
   a. In the row for the scan, click the **menu**.

      The actions menu appears.

   b. Select **Browse**.

      The Vulnerability Summary analysis tool appears, populated with data from the scan.
To view scan result details for a set of scan results:

a. In the row for the scan, click the menu.

The actions menu appears.

b. Click View.

The View Scan Result page appears. For more information, see Scan Result Details.

To retrieve a scan result from a managed Tenable.sc instance:

a. In the row for a Partial or Completed scan that is Not Synced, click the menu. For more information about scan result statuses, see Scan Result Statuses.

The actions menu appears.

b. Click Retrieve.

Tenable.sc Director imports the scan result.

Note: By default, Tenable.sc Director retains scan results from managed Tenable.sc instances for 30 days. For more information, see Data Expiration Settings.

To download the results of a scan:

a. In the row for the scan, click the menu.

The actions menu appears.

b. Select Download.

On a standard scan, you can download a Nessus results file. If the scan contains SCAP results, you can use an additional option to download the SCAP results.

To share scan results with other users:

a. In the row for the scan, click the menu.

The actions menu appears.

b. Select Copy.

Selecting a Group from the drop-down box displays a list of users from that group. You can select one or more users from the list.
To send a copy of the scan results to users without access to Tenable.sc:

a. In the row for the scan, click the menu.
   The actions menu appears.

b. Select Email.

To generate a report for the scan results based off a preconfigured report:

a. In the row for the scan, click the menu.
   The actions menu appears.

b. Select Send to Report.
   Tenable.sc Director sends the scan results to a report.

To upload Nessus scan results performed by other systems:

- See Upload Scan Results.

To pause or resume a running scan:

- In the row for the scan, click the pause or play button, as described in Start or Pause a Scan.

To delete a set of scan results from Tenable.sc Director:

a. In the row for the scan, click the menu.
   The actions menu appears.

b. Select Delete.
   Tenable.sc Director deletes the scan results.
View Scan Results

**Required User Role:** Administrator or organizational user with appropriate permissions. For more information, see [User Roles](#).

For more information, see [Scan Results](#).

To view a list of scan results:

1. Log in to Tenable.sc Director via the user interface.

2. Click **Scan Results** (administrator users) or **Scans > Scan Results** (organizational users).

   The **Scan Results** page appears.

3. View details about each scan result.
   - **Name** — The name for the scan associated with the result.
   - **Tenable.sc Instance** — The name of the Tenable.sc instance where the scan was run.
   - **Type** — The type of scan that generated the scan result.
   - **Scan Policy Plugins** — The name of the scan policy that generated the scan result.
   - **Scanned IPs** — The number of IP addresses scanned.
   - **Group** — The group associated with the scan.
   - **Owner** — The username for the user who added the scan.
   - **Duration** — The total time elapsed while running the scan.
   - **Import Time** — The date and time Tenable.sc completed the scan result import.
   - **Status** — The status of the scan that generated the scan result. For more information, see [Scan Status](#).

4. To retrieve a scan result from a managed Tenable.sc instance, see Retrieve Scan Results.

5. To view additional details for a scan result, see [View Scan Result Details](#).
View Scan Result Details

Required User Role: Administrator or organizational user with appropriate permissions. For more information, see User Roles.

You can view details for any scan result. For more information, see Scan Results.

To view scan result details:

1. Log in to Tenable.sc Director via the user interface.
2. Click Scan Results (administrator users) or Scans > Scan Results (organizational users).
   The Scan Results page appears.
3. In the row for the scan result, click the menu.
   The actions menu appears.
4. Click View.
   The View Scan Result page appears.

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>View general information for the scan result.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Name</strong> — The scan result name.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Type</strong> — The type of scan that generated the scan result.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Tenable.sc Instance</strong> — The name of the Tenable.sc instance where the scan was run.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Scan Policy</strong> — The name of the scan policy that generated the scan result.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Repository</strong> — The name of the repository associated with the scan policy that generated the scan result.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Scanned IPs / Total IPs</strong> — The number of IP addresses scanned compared to the total number of IP addresses targeted in the scan.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Status</strong> — The scan status. For more information, see Scan Status.</td>
</tr>
<tr>
<td>Section</td>
<td>Action</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Start Time</strong></td>
<td>The date and time Tenable.sc started the scan.</td>
</tr>
<tr>
<td><strong>Finish Time</strong></td>
<td>The date and time Tenable.sc completed the scan.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>The scan status. For more information, see <strong>Scan Status</strong>.</td>
</tr>
<tr>
<td><strong>Duration</strong></td>
<td>The total time elapsed while running the scan.</td>
</tr>
<tr>
<td><strong>Import Start</strong></td>
<td>The date and time Tenable.sc started the scan result import.</td>
</tr>
<tr>
<td><strong>Import Finish</strong></td>
<td>The date and time Tenable.sc completed the scan result import.</td>
</tr>
<tr>
<td><strong>Import Status</strong></td>
<td>The scan result import status. For more information, see <strong>Import Status</strong>.</td>
</tr>
<tr>
<td><strong>Import Duration</strong></td>
<td>The total time elapsed during scan result import.</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>The username for the user who added the scan.</td>
</tr>
<tr>
<td><strong>Group</strong></td>
<td>The group associated with the scan.</td>
</tr>
<tr>
<td><strong>ID</strong></td>
<td>The scan result ID.</td>
</tr>
</tbody>
</table>
Solutions Analysis

Tenable provides recommended solutions for all vulnerabilities on your network. You can perform the recommended action in a solution to lower the risk on your network.

For more information, see:

- [View Solutions](#)
- [View Solution Details](#)
View Solutions

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

You can use the **Solutions** page to view solutions for specific assets on your network or drill into solution details.

To view solutions for assets on your network:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Solutions**.
   
The **Solutions** page appears.
3. To filter the solutions in the table by an asset list, in the **Targeted Assets** drop-down box, click an asset list name.
   
The system refreshes the page and filters the table by the asset list you selected. For more information about asset lists, see [Assets](#).
4. View information about each solution.
   
   - **Solution** — A description for the solution.
   
   - **Risk Reduction** — The percent you would reduce your risk by addressing the vulnerability in the solution. Tenable.sc calculates the risk reduction percentage by dividing the score of the vulnerabilities in the solution by the score of all of the vulnerabilities on your network.
   
   - **Hosts Affected** — The number of devices affected by the solution.
   
   - **Vulnerabilities** — The number of vulnerability instances included in the solution.

   **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 highest VPR for a vulnerability included in the solution.
   
   - **CVSSv3 Base Score** — The highest CVSSv3 score for a vulnerability included in the solution. If only CVSSv2 is available, the column is blank.
5. To view details for a solution, click a row.

   The **Solution Details** page appears. For more information, see [Solution Details](#).
View Solution Details

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

You can use the **Solution Details** page to view details for a specific solution.

To view details for a specific solution:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Solutions**.
   
   The **Solutions** page appears.
3. Click a solution row.
   
   The **Solution Details** page appears.

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metrics summary</td>
<td>View summary statistics for the recommended solution.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Hosts Affected</strong> — The number of devices affected by the solution.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Vulnerabilities</strong> — The total number of vulnerability instances included in the solution.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.</td>
</tr>
<tr>
<td></td>
<td>- <strong>VPR</strong> — The highest VPR for a vulnerability included in the solution.</td>
</tr>
<tr>
<td></td>
<td>- <strong>CVSSv3 Base Score</strong> — The highest CVSSv3 score for a vulnerability included in the solution. If only CVSSv2 is available, the column is blank.</td>
</tr>
<tr>
<td>Vulnerabilities Included table</td>
<td>View all vulnerabilities related to the recommended solution, sorted by decreasing VPR.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Plugin</strong> — The plugin ID.</td>
</tr>
<tr>
<td>Section</td>
<td>Action</td>
</tr>
<tr>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hosts Affected</strong> — The number of devices affected by the solution.</td>
</tr>
<tr>
<td></td>
<td>• <strong>VPR</strong> — The VPR for the vulnerability.</td>
</tr>
<tr>
<td></td>
<td>• <strong>CVSSv3 Base Score</strong> — The CVSSv3 score for the vulnerability included in the solution. If only CVSSv2 is available, the column is blank.</td>
</tr>
</tbody>
</table>

**Hosts Affected** table

View device information.

- **IP Address** — The IP address for the device.
- **NetBIOS** — The NetBIOS name, if known.
- **DNS** — The DNS name, if known.
- **OS CPE** — The operating system common platform enumeration (CPE) name.
- **Repository** — The repository name where device's scan data is stored.

A device appears in multiple rows if the device's scan data is stored in multiple repositories.
Vulnerability Analysis

The **Vulnerability Analysis** page displays vulnerabilities from either the cumulative or mitigated vulnerability database. For more information, see [Cumulative vs. Mitigated Vulnerabilities](#).

**Note:** If multiple vulnerabilities share the same **IP Address** or **Agent ID** data, Tenable.sc Director assumes they are from the same host.

To perform a common type of vulnerability analysis, see [View Vulnerabilities by Plugin](#) or [View Vulnerabilities by Host](#).

To view a specific vulnerability analysis tool, see [Vulnerability Analysis Tools](#).
Cumulative vs. Mitigated Vulnerabilities

Tenable.sc stores vulnerabilities in two databases: the cumulative database and the mitigated database. You can choose to view cumulative vulnerabilities or mitigated vulnerabilities in any vulnerability analysis tool. For more information, see View Cumulative or Mitigated Vulnerabilities.

**Cumulative Vulnerabilities**

The cumulative database contains currently vulnerable vulnerabilities, including those that have been recasted, accepted, or previously mitigated.

**Mitigated Vulnerabilities**

The mitigated database contains vulnerabilities that Tenable.sc Director determines are not vulnerable, based on the scan definition, the results of the scan, the current state of the cumulative view, and authentication information.

A vulnerability is mitigated if:

- The IP address of the vulnerability was in the target list of the scan.
- The plugin ID of the vulnerability was in the list of scanned plugins.
- The port of the vulnerability was in the list of scanned ports.
- The vulnerability with that IP address/port/plugin ID combination was not in the scan result.

To start, the vulnerability must be present in the cumulative view to be considered for mitigation. The import process then looks at each vulnerability in the import repository. The import process also verifies that authentication was successful before mitigating any local check vulnerabilities that meet the above criteria.

**Note:** Mitigation logic works with scans using policies defined by templates, advanced policies, and remediation scans. These policies are set up to take advantage of this new mitigation logic.

For more information about mitigation, see the knowledge base article.
View Cumulative or Mitigated Vulnerabilities

Required User Role: Organizational user with appropriate permissions. For more information, see User Roles.

For general information about cumulative vulnerabilities and mitigated vulnerabilities, see Cumulative vs. Mitigated Vulnerabilities.

To switch between viewing mitigated or cumulative vulnerabilities:

1. Log in to Tenable.sc Director via the user interface.
2. Click Analysis > Vulnerabilities.
   - The Vulnerability Analysis page appears.
3. In the upper-right corner, click the Options drop-down menu.
   - The actions menu appears.
4. Click Switch to Mitigated or Switch to Cumulative.
   - The page updates to display data from the mitigated or cumulative vulnerability database.
Severity vs. VPR

Tenable uses a static Severity and a dynamic Vulnerability Priority Rating (VPR) to quantify how urgently you should remediate a vulnerability.

**Note:** When you view these metrics on an analysis page organized by plugin (for example, the Vulnerability Analysis page), the metrics represent the highest value assigned or calculated for a vulnerability associated with the plugin.

Severity

Tenable assigns all vulnerabilities a static severity based on the vulnerability's CVSSv2 or CVSSv3 score.

Severity Categories

Tenable.sc analysis pages provide summary information about vulnerabilities using the following severity categories.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>The plugin's highest vulnerability CVSSv2 score is 10.0.</td>
</tr>
<tr>
<td>High</td>
<td>The plugin's highest vulnerability CVSSv2 score is between 7.0 and 9.9.</td>
</tr>
<tr>
<td>Medium</td>
<td>The plugin's highest vulnerability CVSSv2 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>
</tr>
<tr>
<td>Info</td>
<td>The plugin's highest vulnerability CVSSv2 score is 0.</td>
</tr>
<tr>
<td></td>
<td>- or -</td>
</tr>
<tr>
<td></td>
<td>The plugin does not search for vulnerabilities.</td>
</tr>
</tbody>
</table>

Vulnerability Priority Rating

Tenable calculates a dynamic VPR for most vulnerabilities. The VPR is a dynamic companion to the static data provided by the vulnerability's CVSS score and severity, 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.sc provides new and updated VPR values through the Tenable.sc feed. For more information, see [Edit Plugin and Feed Schedules](#).

Tenable recommends resolving vulnerabilities with the highest VPRs first. You can view VPR scores and summary data in:

- The Tenable-provided [Vulnerability Priority Rating (VPR) Summary](#) dashboard, described in [Dashboards](#).
- The [Vulnerability Summary](#), [Vulnerability List](#), and [Vulnerability Detail List](#) tools, described in [View Vulnerabilities by Plugin](#).

**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><strong>Vulnerability Age</strong></td>
<td>The number of days since the National Vulnerability Database (NVD) published the vulnerability.</td>
</tr>
</tbody>
</table>
| CVSSv3 Impact     | The NVD-provided CVSSv3 impact score for the vulnerability. If the NVD did not provide a score, Tenable.sc displays a Tenable-predicted score.
<table>
<thead>
<tr>
<th>Score</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 Recency</td>
<td>The number of days (0-730) since a threat event occurred for the vulnerability.</td>
</tr>
</tbody>
</table>

### 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
# Vulnerability Analysis Tools

On the **Vulnerability Analysis** page, you can use the drop-down box to select the vulnerability analysis tool you want to view.

To perform a common type of vulnerability analysis, see [View Vulnerabilities by Plugin](#) or [View Vulnerabilities by Host](#).

<table>
<thead>
<tr>
<th>Analysis Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Summary</td>
<td>Summarizes host information, organized by IP address/agent ID. You can click the <strong>IP Address</strong> to view host details, as described in <a href="#">View Host Details</a>. For more information, see <a href="#">View Vulnerabilities by Host</a>.</td>
</tr>
<tr>
<td>Class A Summary</td>
<td>Summarizes host information. The vulnerability score for an address is computed by adding up the number of vulnerabilities at each severity level and multiplying it with the organization’s severity score. Starting out with a Class A or Class B summary can identify more active network ranges for networks with a large number of active IP addresses. You can click a <strong>Class A</strong> or <strong>Class B</strong> row to view the <strong>Class B</strong> or <strong>Class C</strong> tool, filtered by the asset list you selected. You can click a <strong>Class C</strong> row to view the <strong>IP Summary</strong> tool, filtered by the asset list you selected.</td>
</tr>
<tr>
<td>Class B Summary</td>
<td></td>
</tr>
<tr>
<td>Class C Summary</td>
<td></td>
</tr>
<tr>
<td>Asset Summary</td>
<td>This tool summarizes the scores and counts of vulnerabilities for all dynamic or static asset lists. A breakdown of each asset’s specific vulnerabilities and counts for each severity level is also included. You can click a count to view the <strong>IP Summary</strong> tool, filtered by the asset list you selected.</td>
</tr>
<tr>
<td>CCE Summary</td>
<td>This displays a summary of hosts which have Common Configuration Enumeration (CCE) vulnerabilities. You can click a count to view the <strong>Vulnerability Summary</strong> tool, filtered by the CCE vulnerability you selected.</td>
</tr>
<tr>
<td>Analysis Tool</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CVE Summary</td>
<td>This view groups vulnerabilities based on their CVE ID, Hosts Total, and vulnerability count.</td>
</tr>
<tr>
<td>DNS Name Summary</td>
<td>Tenable.sc includes the ability to summarize information by vulnerable DNS name. The DNS Name Summary lists the matching hostnames, the repository, vulnerability count, and a breakdown of the individual severity counts.</td>
</tr>
<tr>
<td></td>
<td>You can click a DNS name to view the <strong>Vulnerability List</strong> tool, filtered by the DNS name you selected.</td>
</tr>
<tr>
<td>List Mail Clients</td>
<td>Tenable.sc uses NNM to determine a unique list of email clients. The list contains the email client name, count of detections, and the detection method.</td>
</tr>
<tr>
<td></td>
<td>You can click a count to view the <strong>IP Summary</strong> tool, filtered by the email client you selected.</td>
</tr>
<tr>
<td>List OS</td>
<td>Tenable.sc understands both actively and passively fingerprinted operating systems. This tool lists what has been discovered.</td>
</tr>
<tr>
<td></td>
<td>The method (active, passive, or event) of discovery is also indicated.</td>
</tr>
<tr>
<td></td>
<td>You can click a count to view the <strong>IP Summary</strong> tool, filtered by operating system.</td>
</tr>
<tr>
<td>List Services</td>
<td>Tenable.sc processes information from scans and creates a summary of unique services discovered. The service discovered, count of hosts, and detection method are listed.</td>
</tr>
<tr>
<td></td>
<td>You can click a service to view the <strong>IP Summary</strong> tool, filtered by the service you selected.</td>
</tr>
<tr>
<td>List SSH Servers</td>
<td>This tool utilizes active and passive scan results to create a unique list of known SSH servers. The list contains the ssh server name, count of detections, and the detection method.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> Not all SSH servers run on port 22. Do not be surprised if you encounter SSH servers running on unexpected ports.</td>
</tr>
<tr>
<td></td>
<td>You can click a count to view the <strong>IP Summary</strong> tool, filtered by the SSH server you selected.</td>
</tr>
<tr>
<td>List Software</td>
<td>Tenable.sc processes information from scans and creates a summary of unique software packages discovered. The software name, count of hosts, and detection</td>
</tr>
</tbody>
</table>

Copyright © 2020 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>Analysis Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>List Web Clients</td>
<td>Tenable.sc understands NNM plugin ID 1735, which passively detects the web client in use. This tool lists the unique web clients detected. The list contains the user-agents, count of detections, and the detection method. You can click a count to view the <strong>IP Summary</strong> tool, filtered by the web client you selected.</td>
</tr>
<tr>
<td>List Web Servers</td>
<td>This tool takes the passive output from passive and active scans to create a unique list of known web servers. The list contains the web server name, count of detections, and the detection method. Tip: Not all web servers run on port 80 or 443. Do not be surprised if you encounter web servers running on unexpected ports. You can click a count to view the <strong>IP Summary</strong> tool, filtered by the web server you selected.</td>
</tr>
<tr>
<td>MS Bulletin Summary</td>
<td>This tool filters vulnerabilities based on Microsoft Bulletin ID. Displayed are the IDs, Vulnerability Totals, Host Total, and Severity. This view is particularly useful in cases where Microsoft releases a new bulletin and a quick snapshot of vulnerable hosts is required.</td>
</tr>
<tr>
<td>Plugin Family Summary</td>
<td>This tool charts the Nessus, NNM, or Event plugin family as well as their relative counts based on severity level for all matching vulnerabilities. You can click a count to view the <strong>Vulnerability List</strong> tool, filtered by the plugin family you selected.</td>
</tr>
<tr>
<td>Port Summary</td>
<td>A summary of the ports in use is displayed for all matched vulnerabilities. Each port has its count of vulnerabilities as well as a breakdown for each severity level. You can click a port to view the <strong>IP Summary</strong> tool, filtered by the port you selected.</td>
</tr>
<tr>
<td>Protocol Summary</td>
<td>This tool summarizes the detected IP protocols such as TCP, UDP, and ICMP. The</td>
</tr>
<tr>
<td>Analysis Tool</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>mary</td>
<td>The <code>mary</code> tool also breaks out the counts for each protocol’s severity levels. You can click a count to view the <strong>IP Summary</strong> tool, filtered by the count you selected.</td>
</tr>
<tr>
<td>Remediation Summary</td>
<td>The Remediation Summary tool provides a list of remediation actions that may be taken to prioritize tasks that have the greatest effect to reduce vulnerabilities in systems. This list provides a solution to resolve a particular CPE on a given OS platform. The data provided includes:</td>
</tr>
<tr>
<td></td>
<td>* <strong>Risk Reduction</strong> — The percent you would reduce your risk by addressing the vulnerability in the solution. Tenable.sc calculates the risk reduction percentage by dividing the score of the vulnerabilities in the solution by the score of all of the vulnerabilities on your network.</td>
</tr>
<tr>
<td></td>
<td>* <strong>Hosts Affected</strong> — The number of unique hosts that would be affected by performing the remediation action.</td>
</tr>
<tr>
<td></td>
<td>* <strong>Vulnerabilities</strong> — The count of vulnerabilities (Nessus plugins) that would be remediated by performing the remediation action.</td>
</tr>
<tr>
<td></td>
<td>* <strong>Score</strong> — This is calculated by adding up the score for each vulnerability that would be remediated by performing the remediation action.</td>
</tr>
<tr>
<td></td>
<td>* <strong>CVE</strong> — The number of distinct CVEs that would be remediated by performing the remediation action.</td>
</tr>
<tr>
<td></td>
<td>* <strong>MS Bulletin</strong> — The number of unique MS Bulletins that would be remediated by performing the remediation action.</td>
</tr>
<tr>
<td></td>
<td>* <strong>Vulnerability %</strong> — The count of vulnerabilities (Nessus plugins) that would be remediated by performing the remediation action over the total vulnerability count returned by the query as a percentage.</td>
</tr>
<tr>
<td>Severity Summary</td>
<td>This tool considers all of the matching vulnerabilities and then charts the total number of info, low, medium, high, and critical vulnerabilities. You can click a count to view the <strong>Vulnerability Summary</strong> tool, filtered by the severity you selected.</td>
</tr>
<tr>
<td>User Responsibility</td>
<td>This displays a list of the users who are assigned responsibility for the vul-</td>
</tr>
</tbody>
</table>

Copyright © 2020 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>Analysis Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Summary</td>
<td>Vulnerability based on the user’s assigned asset list. Multiple users with the same responsibility are displayed on the same line. Users without any assigned responsibilities are not displayed in the list. Tenable.sc populates this list after you assign an asset to a user account.</td>
</tr>
<tr>
<td>Vulnerability Detail List</td>
<td>Displays the details for a specific vulnerability instance on your network.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.</td>
</tr>
<tr>
<td></td>
<td>Important options include CVSS v2/CVSS v3 score, CVSS v2/CVSSv3 temporal score, VPR, VPR key drivers, availability of public exploit, CVE, BID, synopsis, description, and solution.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <a href="#">View Vulnerability Instance Details</a>.</td>
</tr>
<tr>
<td>Vulnerability List</td>
<td>Displays a table of all vulnerability instances found on your network, organized by plugin ID.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <a href="#">View Vulnerabilities by Plugin</a>.</td>
</tr>
<tr>
<td>Vulnerability Summary</td>
<td>Displays a table of all plugins associated with vulnerabilities on your network, organized by plugin ID.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <a href="#">View Vulnerabilities by Plugin</a>.</td>
</tr>
</tbody>
</table>
Vulnerability Analysis Filter Components

For general information about constructing filters, see Filters.

<table>
<thead>
<tr>
<th>Filter Component</th>
<th>Availability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept Risk</td>
<td>Cumulative View</td>
<td>Display vulnerabilities based on their Accepted Risk workflow status. Available choices include Accepted Risk or Non-Accepted Risk. Choosing both options displays all vulnerabilities regardless of acceptance status.</td>
</tr>
<tr>
<td>Address</td>
<td>All</td>
<td>This filter specifies an IPv4 or IPv6 address, range, or CIDR block to limit the viewed vulnerabilities. For example, entering 198.51.100.28/24 and/or 2001:DB8::/32 limits any of the web tools to only show vulnerability data from the selected network(s). Addresses can be comma separated or separate lines.</td>
</tr>
</tbody>
</table>
| Agent ID         | All          | Displays results matching the specified agent UUID (Tenable UUID). An agent UUID uniquely identifies:
- Agent-detected assets that may share a common IP address.
- Tenable.ot assets that may not have an IP address. For more information, see Tenable.ot Instances. |
| Application CPE  | All          | Allows a text string search to match against available CPEs. The filter may be set to search based on a contains, Exact Match, or Regex Filter filter. The Regex Filter is based on Perl-compatible regular expressions (PCRE). |
| Asset            | All          | This filter displays systems from the assets you select. If more than one asset contains the systems from the primary asset (i.e., there is an
<table>
<thead>
<tr>
<th>Filter Component</th>
<th>Availability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>intersect between the asset lists), those assets are displayed as well. The operators <strong>NOT, OR, and AND</strong> may be used to exclude unwanted assets from the view.</td>
<td>Audit File</td>
<td>All</td>
</tr>
<tr>
<td>Displays results matching the entered CCE ID.</td>
<td>CCE ID</td>
<td>All</td>
</tr>
<tr>
<td>Displays vulnerabilities based on one or more CVE IDs. Type multiple IDs as a comma-separated list (e.g., CVE-2011-3348,CVE-2011-3268,CVE-2011-3267).</td>
<td>CVE ID</td>
<td>All</td>
</tr>
<tr>
<td>Displays vulnerabilities within the chosen Common Vulnerability Scoring System version 2 (CVSS v2) score range.</td>
<td>CVSS v2 Score</td>
<td>All</td>
</tr>
<tr>
<td>Filters results based on a search against the CVSS v2 vector information.</td>
<td>CVSS v2 Vector</td>
<td>All</td>
</tr>
<tr>
<td>Displays vulnerabilities within the chosen Common Vulnerability Scoring System version 3 (CVSS v3) score range.</td>
<td>CVSS v3 Score</td>
<td>All</td>
</tr>
<tr>
<td>Filters results based on a search against the CVSS v3 vector information.</td>
<td>CVSS v3 Vector</td>
<td>All</td>
</tr>
<tr>
<td>Filters results based on a search against the cross reference information in a vulnerability.</td>
<td>Cross References</td>
<td>All</td>
</tr>
<tr>
<td>Displays results matching the specified data type: <strong>IPv4, IPv6, or Agent</strong>.</td>
<td>Data Format</td>
<td>All</td>
</tr>
<tr>
<td>This filter specifies a DNS name to limit the viewed vulnerabilities. For example, entering host.example.com limits any of the web tools</td>
<td>DNS Name</td>
<td>All</td>
</tr>
<tr>
<td>Filter Component</td>
<td>Availability</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to only show vulnerability data from that DNS name.</td>
</tr>
<tr>
<td>Exploit Available</td>
<td>All</td>
<td>If set to yes, displays only vulnerabilities for which a known public exploit exists.</td>
</tr>
<tr>
<td>Exploit Frameworks</td>
<td>All</td>
<td>When set, the text option can be equal to or contain the text entered in the option.</td>
</tr>
<tr>
<td>IAVM ID</td>
<td>All</td>
<td>Displays vulnerabilities based on one or more IAVM IDs. Type multiple IDs as a comma-separated list (e.g., <code>2011-A-0005,2011-A-0007,2012-A-0004</code>).</td>
</tr>
<tr>
<td>MS Bulletin ID</td>
<td>All</td>
<td>Displays vulnerabilities based on one or more Microsoft Bulletin IDs. Type multiple IDs as a comma-separated list (e.g., <code>MS10-012,MS10-054,MS11-020</code>).</td>
</tr>
<tr>
<td>Mitigated</td>
<td>All</td>
<td>Display vulnerabilities for a specific mitigation status:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Previously Mitigated</strong> — the vulnerability was previously mitigated but it reappeared in a scan and is currently vulnerable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Not Mitigated</strong> — the vulnerability is currently vulnerable and has never been mitigated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information about mitigation, see <a href="#">Mitigated Vulnerabilities</a>.</td>
</tr>
<tr>
<td>Output Assets</td>
<td>Asset Summary Analysis Tool</td>
<td>This filter displays only the desired asset list systems.</td>
</tr>
<tr>
<td>Patch Published</td>
<td>All</td>
<td>Some plugins contain information about when a patch was published for a vulnerability. This</td>
</tr>
<tr>
<td>Filter Component</td>
<td>Availability</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>filter allows the user to search based on when a vulnerability's patch became available:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>None</strong> (displays vulnerabilities that do not have a patch available)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Within the last day</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Within the last 7 days</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Within the last 30 days</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>More than 7 days ago</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>More than 30 days ago</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Current Month</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Last Month</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Current Quarter</strong> (during the current calendar year quarter)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Last Quarter</strong> (during the previous calendar year quarter)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Custom Range</strong> (during a specific range you specify)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Explicit</strong> (at a specific time you specify)</td>
</tr>
</tbody>
</table>

<p>| Plugin Family    | All          | This filter chooses a Nessus or NNM plugin family. Only vulnerabilities from that family display. |
| Plugin ID        | All          | Type the plugin ID desired or range based on a plugin ID. Available operators are equal to (=), not equal to (!=), greater than or equal (&gt;=) and less than or equal to (&lt;=). |
| Plugin Modified  | All          | Tenable plugins contain information about when a plugin was last modified. This filter |</p>
<table>
<thead>
<tr>
<th>Filter Component</th>
<th>Availability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>allows users to search based on when a particular plugin was modified:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Within the last day</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Within the last 7 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Within the last 30 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- More than 7 days ago</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- More than 30 days ago</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Current Month</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Last Month</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Current Quarter</strong> (during the current calendar year quarter)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Last Quarter</strong> (during the previous calendar year quarter)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Custom Range</strong> (during a specific range you specify)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Explicit</strong> (at a specific time you specify)</td>
</tr>
<tr>
<td>Plugin Name</td>
<td>All</td>
<td>Using the <strong>Contains</strong> option, type all or a portion of the actual plugin name. For example, entering <strong>MS08-067</strong> in the plugin name filter displays vulnerabilities using the plugin named <strong>MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)</strong>. Similarly, entering the string <strong>uncredentialed</strong> displays a list of vulnerabilities with that string in the plugin name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Using the <strong>Regex Match</strong> option regex options</td>
</tr>
<tr>
<td>Filter Component</td>
<td>Availability</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Plugin Published</td>
<td>All</td>
<td>Tenable plugins contain information about when a plugin was first published. This filter allows users to search based on when a particular plugin was created:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Within the last day</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Within the last 7 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Within the last 30 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- More than 7 days ago</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- More than 30 days ago</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Current Month</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Last Month</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Current Quarter (during the current calendar year quarter)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Last Quarter (during the previous calendar year quarter)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Custom Range (during a specific range you specify)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Explicit (at a specific time you specify)</td>
</tr>
<tr>
<td>Plugin Type</td>
<td>All</td>
<td>Select whether to view all plugin types or passive, active, event, or compliance vulnerabilities.</td>
</tr>
<tr>
<td>Port</td>
<td>All</td>
<td>This filter is in two parts. First the equality operator is specified to allow matching vulnerabilities with the same ports, different ports, all ports less than or all ports greater than the port filter. The port filter allows a comma separated list of ports. For the larger</td>
</tr>
<tr>
<td>Filter Component</td>
<td>Availability</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Protocol</td>
<td>All</td>
<td>This filter provides boxes to select TCP, UDP, or ICMP-based vulnerabilities.</td>
</tr>
<tr>
<td>Recast Risk</td>
<td>Cumulative View</td>
<td>Display vulnerabilities based on their Recast Risk workflow status. Available choices include Recast Risk or Non-Recast Risk. Choosing both options displays all vulnerabilities regardless of recast risk status.</td>
</tr>
<tr>
<td>Repositories</td>
<td>All</td>
<td>Display vulnerabilities from the chosen repositories.</td>
</tr>
<tr>
<td>STIG Severity</td>
<td>All</td>
<td>Display vulnerabilities with the chosen STIG severity in the plugins database.</td>
</tr>
<tr>
<td>Scan Policy Plugins</td>
<td>All</td>
<td>Display vulnerabilities found by the currently enabled plugins in the scan policy. For more information, see Plugins Options.</td>
</tr>
<tr>
<td>Severity</td>
<td>All</td>
<td>Displays vulnerabilities with the selected severity. For more information, see Severity vs. VPR.</td>
</tr>
<tr>
<td>Users</td>
<td>All</td>
<td>Allows selection of one or more users who are responsible for the vulnerabilities.</td>
</tr>
<tr>
<td>Vulnerability Discovered</td>
<td>All</td>
<td>Tenable.sc tracks when each vulnerability was first discovered. This filter allows you to see when vulnerabilities were discovered:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Within the last day</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Within the last 7 days</td>
</tr>
</tbody>
</table>

**Note:** All host-based vulnerability checks are reported with a port of 0 (zero).
<table>
<thead>
<tr>
<th>Filter Component</th>
<th>Availability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Within the last 30 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• More than 7 days ago</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• More than 30 days ago</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Current Month</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Last Month</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Current Quarter</strong> (during the current calendar year quarter)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Last Quarter</strong> (during the previous calendar year quarter)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Custom Range</strong> (during a specific range you specify)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Explicit</strong> (at a specific time you specify)</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td></td>
<td>The discovery date is based on when the vulnerability was first imported into Tenable.sc. For NNM, this date does not match the exact vulnerability discovery time as there is normally a lag between the time that NNM discovers a vulnerability and the import occurs.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td></td>
<td>Days are calculated based on 24-hour periods prior to the current time, not calendar days. For example, if the report run time was 1/8/2019 at 1:00 PM, using a 3-day count would include vulnerabilities starting 1/5/2019 at 1:00 PM and not from 12:00 AM.</td>
</tr>
<tr>
<td>Vulnerability Last Observed</td>
<td>Cumulative View</td>
<td>This filter allows the user to see when the vulnerability was last observed by Nessus, LCE, or NNM:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Within the last day</strong></td>
</tr>
<tr>
<td>Filter Component</td>
<td>Availability</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Within the last 7 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Within the last 30 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- More than 7 days ago</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- More than 30 days ago</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Current Month</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Last Month</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Current Quarter</strong> (during the current calendar year quarter)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Last Quarter</strong> (during the previous calendar year quarter)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Custom Range</strong> (during a specific range you specify)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Explicit</strong> (at a specific time you specify)</td>
</tr>
</tbody>
</table>

**Note:** The observation date is based on when the vulnerability was most recently imported into Tenable.sc. For NNM, this date does not match the exact vulnerability discovery as there is normally a lag between the time that NNM discovers a vulnerability and the import occurs.

<table>
<thead>
<tr>
<th>Vulnerability Mitigated</th>
<th>Mitigated View</th>
<th>This filter allows the user to filter results based on when the vulnerability was mitigated:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- Within the last day</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Within the last 7 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Within the last 30 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- More than 7 days ago</td>
</tr>
<tr>
<td>Filter Component</td>
<td>Availability</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Vulnerability Priority Rating (VPR)</td>
<td>All</td>
<td>Displays vulnerabilities within the chosen VPR range. For more information, see <a href="#">Severity vs. VPR</a>.</td>
</tr>
<tr>
<td>Vulnerability Published</td>
<td>All</td>
<td>When available, Tenable plugins contain information about when a vulnerability was published. This filter allows users to search based on when a particular vulnerability was published:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Within the last day</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Within the last 7 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Within the last 30 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• More than 7 days ago</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• More than 30 days ago</td>
</tr>
<tr>
<td>Filter Component</td>
<td>Availability</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Current Month</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Last Month</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Current Quarter</strong> (during the current calendar year quarter)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Last Quarter</strong> (during the previous calendar year quarter)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Custom Range</strong> (during a specific range you specify)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Explicit</strong> (at a specific time you specify)</td>
</tr>
<tr>
<td>Vulnerability Text</td>
<td>All</td>
<td>Displays vulnerabilities containing the entered text (e.g., php 5.3) or regex search term.</td>
</tr>
</tbody>
</table>
View Vulnerabilities by Host

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

You can drill into analysis views, filtering by host, to view vulnerabilities and vulnerability instances on a host.

To view vulnerabilities and vulnerability instances associated with a host:

1. Log in to Tenable.sc Director via the user interface.

2. Click **Analysis** > **Vulnerabilities**.
   
   The **Vulnerability Analysis** page appears.

3. In the drop-down box, click **IP Summary**.
   
   The **IP Summary** tool appears.

4. Filter the tool to locate the host where you want to view vulnerability instance details, as described in [Filters](#) and **Vulnerability Analysis Filter Components**.

5. Click the row for the vulnerability instance where you want to view vulnerability instance details.

   The **Vulnerability List** tool appears, filtered by the vulnerability instance you selected.

   In this tool, you can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td></td>
</tr>
<tr>
<td>menu</td>
<td>Export data as a .csv or a .pdf file, as described in <a href="#">Export Vulnerability Data</a>.</td>
</tr>
<tr>
<td></td>
<td>Save a query, as described in <a href="#">Add or Save a Query</a>.</td>
</tr>
<tr>
<td></td>
<td>Save an asset.</td>
</tr>
<tr>
<td></td>
<td>Open a ticket, as described in <a href="#">Open a Ticket</a>.</td>
</tr>
<tr>
<td></td>
<td>Set the default display columns for the view.</td>
</tr>
<tr>
<td></td>
<td>Set this view as your default view.</td>
</tr>
<tr>
<td></td>
<td>Switch between viewing cumulative vulnerabilities or mitigated vul-</td>
</tr>
</tbody>
</table>
**Filters** sidebar

Apply a filter, as described in [Apply a Filter](#) and [Vulnerability Analysis Filter Components](#).

| Vulnerability row | ・ Click the **Plugin ID** to view the plugin details associated with the vulnerability, as described in [View Plugin Details](#).
| ・ Click the **IP Address** to view the host details for the vulnerability, as described in [View Host Details](#).
| ・ Click the row to view the vulnerability instance details in the **Vulnerability Detail List** tool, as described in [View Vulnerability Instance Details](#). |

**Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.
View Vulnerabilities by Plugin

Required User Role: Organizational user with appropriate permissions. For more information, see User Roles.

You can drill into analysis views, filtering by plugin, to view vulnerabilities and vulnerability instances related to that plugin.

To view vulnerabilities and vulnerability instances associated with a plugin:

1. Log in to Tenable.sc Director via the user interface.

2. Click Analysis > Vulnerabilities.

   The Vulnerability Analysis page appears.

3. In the drop-down box, click Vulnerability Summary.

   The Vulnerability Summary tool appears.

In this tool, you can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options menu</td>
<td>- Export data as a .csv or a .pdf file, as described in Export Vulnerability Data.</td>
</tr>
<tr>
<td></td>
<td>- Save a query, as described in Add or Save a Query.</td>
</tr>
<tr>
<td></td>
<td>- Save an asset.</td>
</tr>
<tr>
<td></td>
<td>- Open a ticket, as described in Open a Ticket.</td>
</tr>
<tr>
<td></td>
<td>- Set the default display columns for the view.</td>
</tr>
<tr>
<td></td>
<td>- Set this view as your default view.</td>
</tr>
<tr>
<td></td>
<td>- Switch between viewing cumulative vulnerabilities or mitigated vulnerabilities, as described in View Cumulative or Mitigated Vulnerabilities.</td>
</tr>
<tr>
<td>Table header</td>
<td>Click the ▼ or ▲ next to a column name to sort the table by that column. Not all columns support sorting.</td>
</tr>
</tbody>
</table>
**Filters side bar**  
Apply a filter, as described in [Apply a Filter](#) and [Vulnerability Analysis Filter Components](#).

**Plugin row**
- Click the **Plugin ID** to view the plugin details for the plugin, as described in [View Plugin Details](#).
- Click the row to view the vulnerability details in the **Vulnerability List** tool.

**Plugin row menu**
View the **DNS Summary** tool or **IP Summary** tool for the plugin.

4. Click the row for the plugin where you want to view vulnerability instance details.

The **Vulnerability List** tool appears, filtered by the plugin you selected.

In this tool, you can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Actions</th>
</tr>
</thead>
</table>
| **Options menu** | • Export data as a `.csv` or a `.pdf` file, as described in [Export Vulnerability Data](#).  
• Save a query, as described in [Add or Save a Query](#).  
• Save an asset.  
• Open a ticket, as described in [Open a Ticket](#).  
• Set the default display columns for the view.  
• Set this view as your default view.  
• Switch between viewing cumulative vulnerabilities or mitigated vulnerabilities, as described in [View Cumulative or Mitigated Vulnerabilities](#). |
| **Filters side bar** | Apply a filter, as described in [Apply a Filter](#) and [Vulnerability Analysis Filter Components](#). |
Vulnerability row

- Click the **Plugin ID** to view the plugin details associated with the vulnerability, as described in **View Plugin Details**.

- Click the **IP Address** to view the host details for the vulnerability, as described in **View Host Details**.

- Click the row to view the vulnerability instance details in the **Vulnerability Detail List** tool, as described in **View Vulnerability Instance Details**.

**Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.
View Vulnerability Instance Details

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

You can drill into analysis views to view details for a specific instance of a vulnerability found on your network.

**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 vulnerability instance details:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Analysis > Vulnerabilities**.
   
   The **Vulnerability Analysis** page appears.
3. In the drop-down box, click **Vulnerability Details List**.
   
   The **Vulnerability Details List** tool appears.

In this tool, you can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options menu</td>
<td>- Export data as a .csv or a .pdf file, as described in <a href="#">Export Vulnerability Data</a>.</td>
</tr>
<tr>
<td></td>
<td>- Save a query, as described in <a href="#">Add or Save a Query</a>.</td>
</tr>
<tr>
<td></td>
<td>- Save an asset.</td>
</tr>
<tr>
<td></td>
<td>- Open a ticket, as described in <a href="#">Open a Ticket</a>.</td>
</tr>
<tr>
<td></td>
<td>- Set this view as your default view.</td>
</tr>
<tr>
<td></td>
<td>- Switch between viewing cumulative vulnerabilities or mitigated vulnerabilities, as described in <a href="#">View Cumulative or Mitigated Vulnerabilities</a>.</td>
</tr>
<tr>
<td>arrows</td>
<td>Click the arrows to view other vulnerability instances related to the plugin.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>toolbar</td>
<td></td>
</tr>
</tbody>
</table>
- Launch a remediation scan, as described in Launch a Remediation Scan.
- Create an accept risk rule, as described in Add an Accept Risk Rule.
- Create a recast risk rule, as described in Add a Recast Risk Rule. |

| **Synopsis and Description** | View information about the plugin, vulnerability instance, and affected assets. |
| **Solution** | View the Tenable-recommended action to remediate the vulnerability. |
| **See Also** | View related links about the plugin or vulnerability. |
| **Discovery** | View details about when the vulnerability was discovered and last seen on your network. |
| **Host Information** | View details about the asset. |
| **Risk Information** | View metrics (e.g., CVSS score, VPR, etc.) about the risk associated with the vulnerability. |
| **Exploit Information** | View details about the exploit. |
| **Plugin Details** | View details about the plugin. |
| **VPR Key Drivers** | View the key drivers Tenable used to calculate the VPR score. For more information, see [Severity vs. VPR](#). |
| **Vulnerability Information** | View Common Platform Enumeration (CPE) details. |
| **Reference Information** | View related links to the CVE, BID, MSFT, CERT, and other industry materials about the vulnerability. |
View Host Details

**Required User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can drill into analysis views to view details for a specific host on your network.

To view host details:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Analysis > Vulnerabilities**.
   
   The **Vulnerability Analysis** page appears.
3. In the drop-down box, click **Vulnerability List**.
   
   The **Vulnerability List** tool appears.
4. In the **IP Address** column, click the icon to view host details for a specific vulnerability instance.

**Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

The host details panel appears.

In this panel, you can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Information</strong></td>
<td>View information about the host system.</td>
</tr>
<tr>
<td><strong>Vulnerabilities</strong></td>
<td>View the number of vulnerabilities on the host, organized by severity category. For more information, see Severity vs. VPR.</td>
</tr>
<tr>
<td><strong>Links</strong></td>
<td>View SANS and ARIN links for the host. If configured, this section also displays custom resource links. Click a resource link to view details for the current IP address/agent IDs. For example, if the current IP address was a publicly registered address, click the ARIN link to view the registration information for that address.</td>
</tr>
<tr>
<td><strong>Assets</strong></td>
<td>View the asset lists containing the asset. For more information, see <a href="#">Assets</a>.</td>
</tr>
</tbody>
</table>
View Plugin Details

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

You can drill into analysis views to view details for a specific instance of a vulnerability found on your network.

**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 plugin details:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Analysis > Vulnerabilities**.
   
   The **Vulnerability Analysis** page appears.
3. In the drop-down box, click **Vulnerability Summary**.
   
   The **Vulnerability Summary** tool appears.
4. In the **Plugin ID** column, click the `i` to view plugin details for a specific plugin.
   
   The **Plugin Details** panel appears.

In this panel, you can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>View information about the plugin, vulnerability instance, and affected assets.</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td>View the Tenable-recommended action to remediate the vulnerability</td>
</tr>
<tr>
<td><strong>Vulnerability Priority Rating (VPR) Key Drivers</strong></td>
<td>View the key drivers Tenable used to calculate the vulnerability VPR. For more information, see <a href="#">Severity vs. VPR</a>.</td>
</tr>
<tr>
<td><strong>CVE and BID</strong></td>
<td>View related links to the CVE and BID materials about the vulnerability</td>
</tr>
<tr>
<td>Cross-References</td>
<td>View related documentation for the vulnerability.</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>See Also</td>
<td>View related links about the plugin or vulnerability.</td>
</tr>
</tbody>
</table>
Export Vulnerability Data

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

You can export data from the Vulnerability Analysis page as a `.csv` or a `.pdf` file.

To export data from the Vulnerability Analysis page:

1. Log in to Tenable.sc Director via the user interface.

2. Click **Analysis > Vulnerabilities**.

   The Vulnerability Analysis page appears.

3. In the upper-right corner, click the **Options** drop-down box.

4. Click **Export as CSV** or **Export as PDF**.

   **Note:** If the record count (rows displayed) of any CSV export is greater than 1,000, Tenable.sc Director prompts you for the name of the CSV report you want to generate. After generation, you can download the report from the **Report Results** page.

5. Select or clear the check boxes to indicate which columns you want to appear in the exported file.

6. Click **Submit**.

   Tenable.sc Director exports the vulnerability data.
Reports

Tenable provides extremely flexible and simplified reporting through an assortment of report templates and user-friendly report creation interface. Supported report types include the well-known Portable Document Format (PDF), Rich Text Format (RTF), and Comma-Separated Values (CSV) standards for a high level of compatibility and ease of use.

In Tenable.sc Director, organizational users can create custom reports or template-based reports, as described in Create a Custom Report or Create a Template Report.

**Tip:** Tenable provides many report templates (e.g., the Executive VPR Summary Report) through the Tenable.sc feed. For a complete index of Tenable-provided report templates, see the Tenable.sc Reports blog.

**Note:** Custom PDF reports and template-based reports require that either the Oracle Java JRE or OpenJDK (along with their accompanying dependencies) are installed on the system hosting the Tenable.sc.

Custom CyberScope, DISA ASR, DISA ARF, and DISA Consolidated ARF reports are also available for specialized needs. An administrator user must enable report generation options before organizational users can generate reports with CyberScope, DISA ASR, DISA ARF, or DISA Consolidated ARF data.

To manage reports on the Reports page, see Manage Reports.
Manage Reports

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

On the **Reports** page of Tenable.sc, you can manage report definitions and launch reports.

To manage reports:

1. Click **Reporting > Reports**.
   
   The **Reports** page appears.

2. You can:
   
   - [Filter existing report definitions in the reports table](#).
   - [Create a custom report](#).
   - [Create a template report](#).
   - [Edit a report definition](#).
   - [Edit a report outline](#).
   - [Manage filters for a chapter report](#).
   - [Manage filters for a non-chapter report](#).
   - [View a report definition](#).
   - [Copy a report definition](#).
   - [Export a report definition](#).
   - [Import a report definition](#).
   - [Delete a report definition](#).
   - [Launch a report on demand](#).
   - [Add a report to a scan](#).
Create a Custom Report

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

Before you begin:

- If you want to create a CyberScope, DISA ASR, DISA ARF, or DISA Consolidated ARF report, confirm an administrator user enabled report generation options as described in [Configuration Settings](#).
- If you want to create a CyberScope, DISA ARF, or DISA Consolidated ARF report, create report attributes as described in [CyberScope and DISA Report Attributes](#).

To create a custom report definition:

1. Log in to Tenable.sc via the user interface.
2. Click **Reporting > Reports**.
   
The **Reports** page appears.
3. Click **Add**.
   
The **Add Report** page appears.

4. In the **Custom** section, click the icon corresponding type of the report you want to create:
   
   - **PDF** — Portable Document Format (PDF); can be viewed universally.
   - **CSV** — Comma Separated Values (CSV); can be imported into spreadsheets or databases.
   - **RTF** — Rich Text Format (RTF); can be viewed and edited in any text editor.
   - **DISA ARF** — Meets the standards of the Defense Information Systems Agency (DISA) Assessment Results Format (ARF).
   - **DISA ASR** — Meets the standards of the Defense Information Systems Agency (DISA) Assessment Summary Results (ASR).
   - **DISA Consolidated ARF** — Meets the standards of the Defense Information Systems
Agency (DISA) Consolidated Assessment Results Format (ARF)

- **CyberScope** — Meets CyberScope reporting standards to support FISMA compliance.

5. **Configure the options** for the report.

   Tenable.sc displays options relevant to the report format you selected.

6. (Optional) **Edit the report outline**.

7. Click **Submit** to save your report.
Create a Template Report

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

Template reports are formatted reports that can be customized using chapter and target selections. For more information, see [Reports](#).

To create a template report:

1. Log in to Tenable.sc via the user interface.
2. Click **Reporting > Reports**.
   
   The **Reports** page appears.

3. Click **Add**.
   
   The **Add Report** page appears.

4. In the **Search Templates** box in the top right corner of the page, search for a specific template by keyword.

   **Tip:** After the initial search, you can limit search results by template category.

   -or-

   In the **Template** section, click a template category to view the related templates:
   
   - Compliance & Configuration Assessment
   - Discovery & Detection
   - Executive
   - Monitoring
   - Security Industry Trends
   - Threat Detection & Vulnerability Assessments

5. Click a template report to select it.
6. (Optional) In the **Chapters** section, select which chapters from the template you want to include in your report. By default, the report includes all chapters from the template.

7. In the **Focus** section, do one of the following:

   **Target all systems in the report.**

   * **Note:** This is the default setting.

   To return to this setting, click **All Systems** in the **Targets** drop-down box.

   **Target specific assets in the report.**

   a. In the **Targets** drop-down box, click **Assets**.

   b. Select **Assets** and **Repositories**.

   **Target specific IP addresses in the report.**

   a. In the **Targets** drop-down box, click **IP Addresses**.

   b. In the **IP Addresses** box, type the IP address or addresses where you want the report to focus. Use commas to separate multiple addresses.

   c. In the **Repositories** box, select a target repository or repositories.

   **Target specific repositories in the report.**

   a. In the **Targets** drop-down box, click **Repositories**.

   b. In the **Repositories** box, select a target repository or repositories.

8. (Optional) Edit the default text in the **Description** box.

   * **Note:** You cannot modify any information in the **Details** section of the page.

9. Click **Add**.

    Tenable.sc creates a report based on the template and displays the **Reports** page. The new report appears as the last entry in reports table.
10. (Optional) **Modify report options** that are common to both custom and template reports.

    For example, the default value for the **Schedule** option for all template-based reports is **On Demand**. If you want to run the report automatically, modify the **Schedule** option for the report.

11. (Optional) **Edit the report outline**.

    For example, you might want to use text elements to add your business context to template-based chapters.
Data Required for Template-Based Reports

Each report template description contains icons that represent which types of data must be available on Tenable.sc to obtain a complete report.

Hover the cursor over the icon to display the label.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Label</th>
<th>Action Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>🗂️</td>
<td>Asset Required</td>
<td>Configure an IPv4/IPv6 repository and store scan results in the repository; see Local Repositories and.</td>
</tr>
<tr>
<td>📝</td>
<td>Audit File Required</td>
<td>Upload audit files and add them to your scan policy; see Audit Files and Scan Policies.</td>
</tr>
<tr>
<td>🔑</td>
<td>Local Checks Required</td>
<td>Configure and run credentialed scans; see Active Scans.</td>
</tr>
<tr>
<td>📱</td>
<td>Mobile Data Required</td>
<td>Configure a mobile repository and store scan results in the repository; see Mobile Repositories.</td>
</tr>
<tr>
<td>🌈</td>
<td>Active Data Required</td>
<td>Configure a Nessus scanner and run active scans. For more information, see Nessus Scanners and Active Scans.</td>
</tr>
<tr>
<td>🌟</td>
<td>Passive Data Required</td>
<td>Configure a Nessus Network Monitor (NNM) scanner; see Nessus Network Monitor (PVS).</td>
</tr>
<tr>
<td>📑</td>
<td>Event Data Required</td>
<td>Configure a Log Correlation Engine server; see Log Correlation Engines.</td>
</tr>
</tbody>
</table>
Edit a Report Definition

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

In Tenable.sc, you can edit both custom reports and reports based on templates.

To edit a report definition:

1. Click **Reporting > Reports**.
   
   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.
   
   The **Edit Report** page appears.

3. **Modify the report options**.
   
   **Note:** Tenable.sc displays options relevant to the report type.

4. (PDF, RTF, and template reports only) **Edit the report outline**.

5. Click **Submit** to save your changes to the report.
Report Options

In Tenable.sc, you can configure the options described below for both custom and template reports.

Option descriptions below are grouped by the section where they appear in the Add Report and Edit Report pages. In the option description tables, the Relevant Reports column specifies which report types use each option.

**Note:** Tenable.sc classifies a template-based report as a PDF report. You can configure the same options for that report as you can for a PDF report. During template report creation, Tenable.sc set these options to default values. You can change these options for a template report only after creation is complete.

- **General Options**
- **Report Options**
- **Definition Options**
- **Display Options**
- **Distribution Options**

### General Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Relevant Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name assigned to the report.</td>
<td>Any</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive text for the report.</td>
<td>Any</td>
</tr>
<tr>
<td>Schedule</td>
<td>Determines how often the report runs. Options are <strong>On Demand</strong>, <strong>Now, Once, Daily, Weekly</strong>, or <strong>Monthly</strong>. When you select a frequency from the drop-down box, Tenable.sc displays additional options for the selected time frame.</td>
<td>Any</td>
</tr>
<tr>
<td>Attribute Sets</td>
<td>Predefined operational attributes that add required information to DISA ARF, DISA Consolidated ARF, or CyberScope report types. The drop-down box displays only the attribute set defined for the report you are currently creating.</td>
<td>DISA ARF, DISA Consolidated ARF, Cyber-</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Relevant Reports</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td><strong>ASR Content</strong></td>
<td>When creating a report, this drop-down box offers a selection of Benchmark, IAVM, CVE, or Plugin ID to be included.</td>
<td>DISA ASR, DISA Consolidated ARF</td>
</tr>
<tr>
<td><strong>ASR Record Format</strong></td>
<td>This drop-down box determines the format (Summary or Detail) of the DISA ASR report.</td>
<td>DISA ASR</td>
</tr>
<tr>
<td><strong>Include ARF</strong></td>
<td>When enabled, allows for the inclusion of a DISA attribute set for the report.</td>
<td>DISA ASR</td>
</tr>
<tr>
<td><strong>Benchmarks</strong></td>
<td>Benchmarks are generated after a scan using certain audit files that have been successfully run against at least one target system.</td>
<td>DISA ASR, DISA Consolidated ARF, Cyber-Scope</td>
</tr>
</tbody>
</table>

### Report Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Relevant Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Style</strong></td>
<td>A compound value that specifies the report style, paper size, and orientation. For example, <strong>Plain, Letter</strong></td>
<td>PDF, RTF</td>
</tr>
</tbody>
</table>

Report styles include:

- Plain — a report with basic graphs
- Tenable — a report with basic graphs and a [footer logo](#) on the cover page
- Tenable 3D — a report with enhanced 3D graphs and a [footer logo](#) on the cover page

**Note:** If an administrator configured a Classification Type banner, plain report styles are the only options listed.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Relevant Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper sizes</td>
<td>Paper sizes include:</td>
<td></td>
</tr>
</tbody>
</table>
|                   | - Letter—the standard 8.5 inches x 11 inches letter size  
|                   |   - A4—the standard 8.27 inches x 11.69 inches A4 size  
| Note:            | Letter size is the default paper size, used by options that do not explicitly state a paper size. For example, the paper size for **Plain, Landscape** is letter size. |                   |
| Orientation options| Orientation options include:                                                                                                                                                                               |                   |
|                   | - Portrait—horizontal  
| Note:            | Portrait is the default orientation, used by options that do not explicitly state an orientation. For example, the orientation for **Plain, Letter** is horizontal.                                              |                   |
|                   | - Landscape—vertical   |
| Include Cover Page| Include a cover page in the report. Cover pages include:                                                                                                                                                   | PDF, RTF          |
|                   |   - a [cover logo](#)  
|                   |   - the scan [Name](#)  
|                   |   - the date and time you generated the report  
|                   |   - the date and time Tenable.sc imported the scan results, if you generated the report from scan results  
|                   |   - the scan result [ID](#), if you generated the report from scan results  |
| Include Header    | Include a predefined header in the report.                                                                                                                                                               | PDF               |
| Include Footer    | Include a predefined footer in the report.                                                                                                                                                              | PDF               |
| Include Table of  | Include a table of contents with the report.                                                                                                                                                           | PDF, RTF          |
### Option | Description |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contents</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Include Index</strong></td>
<td>Include an Index with the report.</td>
</tr>
<tr>
<td><strong>Cover Logo</strong></td>
<td>Specifies which image to use for the lower-left footer logo on the cover page of the report. The default logo is the Tenable logo. To add a custom logo, see <a href="#">Report Images</a>.</td>
</tr>
<tr>
<td><strong>Footer Logo</strong></td>
<td>Specifies which image to use for the lower-left footer logo on all pages except the cover page. The default logo is the Tenable logo. To add a custom logo, see <a href="#">Report Images</a>.</td>
</tr>
<tr>
<td><strong>Watermark</strong></td>
<td>Specifies a watermark for each page of the report. The default watermark is no watermark. To add a custom watermark, see <a href="#">Report Images</a>.</td>
</tr>
<tr>
<td><strong>Encrypt PDF</strong></td>
<td>Protect the PDF with a password. The encryption level is 40-bit RC4. When enabled, a password option is displayed for a text entry of a password to use. This password must be used to open the report and view its contents. For more information about this encryption mechanism, please refer to the following URL: <a href="https://xmlgraphics.apache.org/fop/1.0/pdrencryption.html">https://xmlgraphics.apache.org/fop/1.0/pdrencryption.html</a>.</td>
</tr>
</tbody>
</table>

### Definition Options

Tenable.sc displays definition options relevant to the report or report element type.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add Chapter</strong></td>
<td>The primary component in the report organization. Chapters are listed in the table of contents for the report and consist of sections and elements. For more information, see <a href="#">Add a Custom Chapter to a</a>.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Add Template Chapter</strong></td>
<td>A predefined chapter from a Tenable-provided report template. For more information, see Add a Template Chapter to a Report.</td>
</tr>
<tr>
<td><strong>Query</strong></td>
<td>A list of predefined queries you can use to retrieve data for the report. For more information, see Queries.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>The type of data to include in the report.</td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>The source of the data to include in the report. For CSV reports, valid values for this field differ based on the setting of the Type option:</td>
</tr>
<tr>
<td></td>
<td>- If <strong>Type</strong> is set to Vulnerability, valid Source values are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Cumulative</strong>—All vulnerabilities, regardless of whether the vulnerabilities have been remediated or not</td>
</tr>
<tr>
<td></td>
<td>- <strong>Mitigated</strong>—Remediated vulnerabilities</td>
</tr>
<tr>
<td></td>
<td>- <strong>Individual Scan</strong>—Vulnerabilities identified in a specific scan</td>
</tr>
<tr>
<td><strong>Note:</strong> If you select Individual Scan, Tenable.sc displays the Selected Scan option, which allows you to select a scan to use as the basis of the report:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. Click one of the predefined date ranges, or click <strong>Custom Range</strong></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>and enter starting and ending days for the range.</td>
</tr>
<tr>
<td></td>
<td>b. Click <strong>Fetch Scans</strong> to view a list of possible scans within the date range.</td>
</tr>
<tr>
<td></td>
<td>c. Click the scan you want to use in the drop-down box.</td>
</tr>
</tbody>
</table>

- **If** **Type** **is set to Event**, valid **Source** values are:
  - **Active**—Currently active events
  - **Archive**—Archived events

  **Note:** If you select **Archive**, Tenable.sc displays additional options, allowing you to select the **LCE** that collected the events and the **Silo** that stores the archived events.

- **If** **Type** **is set to Mobile**, Ticket, or Alert, this option is absent.

For DISA ARF, DISA Consolidated ARF, and DISA ASR reports, you do not set the **Type** option. Valid **Source** values are limited to **Cumulative** and **Individual Scan**, which operate in the same way as they do for CSV reports.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Select the tool Tenable.sc uses to analyze the data in the report.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Filters</th>
<th>Specifies additional criteria to refine report data. For more information, see <strong>Manage Filter Components for a Non-Chapter Report</strong>.</th>
</tr>
</thead>
</table>

| CSV; Iterator, Table, and Chart elements in PDF and RTF |
| CSV, DISA ARF, DISA Consolidated ARF, DISA ASR, CyberScope; Iterator, Table, and Chart elements in PDF and RTF |
### Display Options

These options allow you to specify column format information format. A selection to define the columns and number of results to appear in the report is then available for configuration.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Relevant Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Find/Update Filters</strong></td>
<td>This option appears after you add at least one chapter to the report. For more information, see Manage Filter Components for Multiple Elements.</td>
<td>PDF, RTF</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Relevant Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Results Displayed</strong></td>
<td>The number of results included in the CSV file.</td>
<td>CSV; Iterator, Table, Bar Chart, and Pie Chart elements in PDF and RTF</td>
</tr>
</tbody>
</table>
| **Sort Column** | The column that Tenable.sc uses to sort results in the CSV file. Available columns depend on:  
- the **Type** you selected in the **Definition** options  
- the **Display Columns** value you select in the **Display** options | CSV; Iterator, Table, Bar Chart, and Pie Chart elements in PDF and RTF |
| **Sort Direction** | The sort direction for results in the CSV file. | CSV; Iterator, Table, Bar Chart, and Pie Chart elements in PDF and RTF |
| **Display Columns** | The columns included in the CSV results file. Available columns depend on **Definition** options you select. | CSV; Iterator, Table, Bar Chart, and Pie Chart elements in PDF and RTF |

### Distribution Options

Distribution options specify the actions Tenable.sc takes when a report run completes.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Relevant Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Users</td>
<td>Allows you to select Tenable.sc users to whom Tenable.sc emails the completed report. The drop-down list includes only users with defined email addresses.</td>
<td>Any</td>
</tr>
<tr>
<td>Email Addresses</td>
<td>Allows you to add email addresses where Tenable.sc emails the completed report. You can specify multiple email addresses, separated by commas.</td>
<td>Any</td>
</tr>
<tr>
<td>Share</td>
<td>Allows you to select which Tenable.sc users within your organization can view the completed report in Tenable.sc. Use this option if organizational policies prohibit emailing potentially sensitive data.</td>
<td>Any</td>
</tr>
<tr>
<td>Publishing Sites</td>
<td>Allows you to select predefined publishing sites where Tenable.sc uploads the completed report. For more information, see <a href="#">Publishing Sites Settings</a>.</td>
<td>Any</td>
</tr>
</tbody>
</table>
Edit a Report Outline

Required User Role: Organizational user with appropriate permissions. For more information, see User Roles.

In Tenable.sc, the report outline allows you to modify the structure of a PDF, RTF, or template-based report.

The outline consists of the following components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Outline Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>chapter</td>
<td>primary</td>
<td>Highest-level component. Can contain any type of element (grouping, text, chart).</td>
</tr>
<tr>
<td>element</td>
<td>subordinate</td>
<td>A grouping, text, or chart element. Can be nested in a chapter or grouping component.</td>
</tr>
</tbody>
</table>

To edit a report outline:

1. Click Reporting > Reports.
   The Reports page appears.

2. In the reports table, click the name of the report you want to edit.
   The Edit Report page appears.

3. In the left navigation bar, click Definition.
   The report outline appears. The outline is, by default, expanded.

4. In the report outline, you can:
   - Expand or collapse elements nested in the outline by clicking Collapse All or Expand All in the top navigation bar.
   - Expand or collapse elements nested in an individual chapter or element by clicking the arrow next to the element.
   - Add a custom chapter.
- Add a template chapter.
- Add or edit a report element.
- Reorder chapters and elements in a report.
- Delete a report element by clicking the delete icon next to the element.

**Note:** Tenable.sc does not ask you to confirm this deletion. However, the deletion is not final until you save all changes to the report.

5. Click **Submit** to save your changes to the report.
Add a Custom Chapter to a Report

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

In Tenable.sc, you can add custom chapters to PDF, RTF, or template-based reports.

To add a custom chapter to a report definition:

1. Click **Reporting > Reports**.
   
   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.
   
   The **Edit Report** page appears.

3. In the left navigation bar, click **Definition**.
   
   The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).

4. In the bottom navigation bar of the report outline, click **Add Chapter**

   **Tip:** If the report contains multiple chapters or sections, scroll down to locate the bottom navigation bar. It can also be helpful to click **Collapse All** on the top navigation bar to collapse the outline to its highest-level components.

   The **Add Chapter** page appears.

5. In the **Name** box, enter a title for the chapter.

6. In the **Location** box, select a relative location for the chapter within the report.

7. In the **Style** box, select a style for the report.

8. Click **Submit**.
   
   Tenable.sc adds the chapter to the report and displays the **Edit Report** page.

9. Click **Submit** to save your changes to the report.
Add a Template Chapter to a Report

**Required User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

In Tenable.sc, you can add template chapters to template reports and custom PDF or RTF reports.

To add a template-based chapter to a report definition:

1. Click **Reporting > Reports**.
   
The Reports page appears.

2. In the reports table, click the name of the report you want to edit.
   
The Edit Report page appears.

3. In the left navigation bar, click **Definition**.
   
The report outline appears. This outline is, by default, expanded. For more information, see Edit a Report Outline.

4. In the top navigation bar of the outline, click **Add Template Chapter**.

5. Do one of the following:
   
   - In the **Search Templates** box in the top right corner of the page, search for a specific template by keyword.

   **Tip:** After the initial search, you can limit search results by template category.

   - Click a template category icon to view the related templates.

6. Click the report template that contains chapters you want to include in your custom report.

7. (Optional) Modify the default options for the report template:
   
   a. In the **Chapters** section, select which chapters from the template you want to include in your report. By default, the report includes all chapters from the template.
b. Do one of the following:

- In the **Focus** section, target all systems in the report.
  
  This is the default setting. To return to this setting, click **All Systems** in the **Targets** drop-down box.

- Target specific assets in the report.
  
  i. In the **Targets** drop-down box, click **Assets**.
  
  ii. Select **Assets** and **Repositories**.

- Target specific IP addresses in the report.
  
  i. In the **Targets** drop-down box, click **IP Addresses**.
  
  ii. In the **IP Addresses** box, type the IP address or addresses where you want the report to focus. Use commas to separate multiple addresses.
  
  iii. In the **Repositories** box, select a target repository or repositories.

- Target specific repositories in the report.
  
  i. In the **Targets** drop-down box, click **Repositories**.
  
  ii. In the **Repositories** box, select a target repository or repositories.

c. (Optional) Edit text in the **Description** box.

**Note:** You cannot modify any information in the **Details** section.

8. Click **Add**.

Tenable.sc adds the template chapter or chapters to your custom report and displays the **Add Report** page again.

9. (Optional) Change the template chapter options.

a. Click the edit icon next to the chapter you added.

b. In the **Name** box, edit the chapter title.

c. In the **Location** box, change the relative location for the chapter within the report.
d. In the **Style** box, select a style for the chapter.

e. Click **Submit** to save your changes to the chapter.

10. Click **Submit** to save your changes to the report.
Add or Edit a Report Element

**Required User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can add or edit elements within chapters or grouping elements in Tenable.sc reports.

To add or edit a report element:

1. Click **Reporting > Reports**.
   - The Reports page appears.

2. In the reports table, click the name of the report you want to edit.
   - The Edit Report page appears.

3. In the left navigation bar, click **Definition**.
   - The report outline appears. This outline is, by default, expanded. For more information, see Edit a Report Outline.

4. Do one of the following:
   - Click **Add Element** next to the element where you want to add the element.
   - Click the edit icon next to the element you want to change.

   **Tip:** To display Add Element or the edit icon, hover the cursor over the element.

5. Configure any of the following types of elements:
   - **Grouping**
   - **Text**
   - **Charts**

6. Click **Submit** to save your changes to the report.
Configure a Grouping Element in a Report

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

Grouping elements in Tenable.sc reports include:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Relevant Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Groups associated elements on the same page.</td>
<td>PDF, RTF</td>
</tr>
<tr>
<td>Section</td>
<td>Allows you to organize content within chapters.</td>
<td>PDF, RTF</td>
</tr>
<tr>
<td>Iterator</td>
<td>Allows you to specify how the report groups its data. For example, if an Iterator Type of Port Summary is chosen for a vulnerability report, vulnerability data in the report is grouped by detected ports. If you do not configure an iterator, hosts and vulnerabilities are listed in the report individually.</td>
<td>PDF, RTF</td>
</tr>
</tbody>
</table>

To configure a grouping element:

1. Click **Reporting > Reports**.
   - The **Reports** page appears.
2. In the reports table, click the name of the report you want to edit.
   - The **Edit Report** page appears.
3. In the left navigation bar, click **Definition**.
   - The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).
4. Click **Add Element**.

**Tip:** To display **Add Element**, hover the cursor over the element.
5. Do one of the following:

- Add a group to the report.
  a. In the **Grouping** section, click the **Group** icon.
  b. Configure the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name for the element.</td>
</tr>
<tr>
<td>Location</td>
<td>Select a location for the element in the report.</td>
</tr>
<tr>
<td>Style</td>
<td>Select a style for the element.</td>
</tr>
</tbody>
</table>

- Add a section to the report.
  a. In the **Grouping** section, click the **Section** icon.
  b. Configure the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name for the element.</td>
</tr>
<tr>
<td>Location</td>
<td>Select a location for the element in the report.</td>
</tr>
<tr>
<td>Style</td>
<td>Select a style for the element.</td>
</tr>
</tbody>
</table>

- Add an iterator to the report.
  a. In the **Grouping** section, click the **Iterator** icon.
  b. Configure the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type a name for the element.</td>
</tr>
<tr>
<td>Location</td>
<td>Select a location for the element in the report.</td>
</tr>
<tr>
<td><strong>Style</strong></td>
<td>Select a style for the element.</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td><strong>Definition</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Query</strong></td>
<td>Select a predefined query to define the data included in the element. For more information, see Queries.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Select the type of data to include in the element. Iterator elements support vulnerability or event data only.</td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>Select the source of the data included in the element. Valid values for this field differ based on the setting of the <strong>Type</strong> option:</td>
</tr>
<tr>
<td></td>
<td>• If <strong>Type</strong> is set to <strong>Vulnerability</strong>, valid <strong>Source</strong> values are:</td>
</tr>
<tr>
<td></td>
<td>◦ <strong>Cumulative</strong>—All vulnerabilities, regardless of whether the vulnerabilities have been remediated or not</td>
</tr>
<tr>
<td></td>
<td>◦ <strong>Mitigated</strong>—Remediated vulnerabilities</td>
</tr>
<tr>
<td></td>
<td>◦ <strong>Individual Scan</strong>—Vulnerabilities identified in a specific scan</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you select <strong>Individual Scan</strong>, Tenable.sc displays the <strong>Selected Scan</strong> option, which allows you to select a scan to use as the basis of the report:</td>
</tr>
<tr>
<td></td>
<td>a. Click one of the predefined date ranges, or click <strong>Custom Range</strong> and enter starting and ending days for the range.</td>
</tr>
<tr>
<td></td>
<td>b. Click <strong>Fetch Scans</strong> to view a list of possible scans within the date range.</td>
</tr>
<tr>
<td></td>
<td>c. Click the scan you want to use in the drop-down box.</td>
</tr>
<tr>
<td></td>
<td>• If <strong>Type</strong> is set to <strong>Event</strong>, valid <strong>Source</strong> values are:</td>
</tr>
</tbody>
</table>
- **Active**—Currently active events
- **Archive**—Archived events

**Note:** If you select **Archive**, Tenable.sc displays additional options, allowing you to select the **LCE** that collected the events and the **Silo** that stores the archived events.

### Filters
Specify additional criteria to refine element data. See [Manage Filters for a Chapter Report](#).

### Iterator Type
Select a grouping method for iteration data:
- **IP Summary**—Group vulnerability or event data by the IP addresses of detected hosts.
- **Port Summary**—Group vulnerability or event data by the detected ports.
- **Type Summary**—Group event data by event type.
- **User Summary**—Group event data by user.
- **Vulnerability Summary**—Group vulnerability data by individual vulnerability.

### Results Displayed
Select the number of results you want to include in the iteration.

### Sort Column
Select the column that Tenable.sc uses to sort the iteration data.

### Sort Direction
Select the sort direction for the iteration data.

### Header Information
Select the columns you want to include in the iteration data. Available columns depend on the settings of the **Type** and **Source** options.

6. Click **Submit** to save the element.

7. Click **Submit** to save your changes to the report.
Configure a Text Element in a Report

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

Text elements in Tenable.sc reports include:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Relevant Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Matrix</td>
<td>Data in a chart layout.</td>
<td>PDF, RTF</td>
</tr>
<tr>
<td>Table</td>
<td>Data in a table layout (max results displayed: 999). The underlying data set determines the report display. The default view for most reports is host-centric and Tenable.sc presents the user with the ability to choose a vulnerability-centric report (a listing of vulnerabilities with all associated hosts).</td>
<td>PDF, RTF</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Descriptive text that can be inserted anywhere in the report. Use this option to describe table elements or report output for the viewer.</td>
<td>PDF, RTF</td>
</tr>
<tr>
<td>Assurance Report Card</td>
<td>An element based on the results of a selected Assurance Report Card.</td>
<td>PDF, RTF</td>
</tr>
</tbody>
</table>

To configure a text element in a report:

1. Click **Reporting > Reports**.
   
   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.
   
   The **Edit Report** page appears.

3. In the left navigation bar, click **Definition**.
   
   The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).

4. Do one of the following:
• Click **Add Element** to add an element.

• Click the edit icon next to the element to edit an existing element.

**Tip:** To display **Add Element** and the edit icon, hover the cursor over the element.

5. Do one of the following:

• **Add a matrix to the report.**

• **Add a table to the report.**

• **Add a paragraph to the report.**
  
  a. In the **Text** section, click the **Paragraph** icon.

  b. Configure the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name for the element.</td>
</tr>
<tr>
<td>Location</td>
<td>Select a location for the element in the report.</td>
</tr>
<tr>
<td>Style</td>
<td>Select a style for the element.</td>
</tr>
<tr>
<td>Text</td>
<td>Type the text of the paragraph.</td>
</tr>
</tbody>
</table>

  c. Click **Submit** to save your changes to the element.

• **Add an assurance report card to the report.**
  
  a. In the **Text** section, click the **Assurance Report Card** icon.
b. Configure the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name for the element.</td>
</tr>
<tr>
<td>Location</td>
<td>Select a location for the element in the report.</td>
</tr>
<tr>
<td>Style</td>
<td>Select a style for the element.</td>
</tr>
<tr>
<td>Assurance Report Card</td>
<td>Select the Assurance Report Card (ARC) you want to add to the report. For more information on ARCs, see <a href="https://example.com">Assurance Report Cards</a>.</td>
</tr>
</tbody>
</table>

c. Click **Submit** to save your changes to the element.

6. Click **Submit** to save your changes to the report.
Configure a Matrix Element in a Report

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

A matrix element is a type of text element you can insert into a Tenable.sc report definition. For more information on text elements, see [Configure a Text Element in a Report](#).

To configure a matrix element in a report:

1. Click **Reporting > Reports**.
   
The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.
   
The **Edit Report** page appears.

3. In the left navigation bar, click **Definition**.
   
The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).

4. Do one of the following:
   
   - **Add a new element.**
     
     a. Click **Add Element**.
     
     b. In the **Text** section, click the **Matrix** icon.
     
     - Click the edit icon next to the element you want to change.

   **Tip:** To display **Add Element** and the edit icon next to an element, hover the cursor over the element.

5. Configure the **General** options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name for the element.</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Select a location for the element in the report.</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td><strong>Style</strong></td>
<td>Select a style for the element.</td>
</tr>
</tbody>
</table>

6. In the **Cells** section, select the number of columns and rows you want the matrix to include. By default, the matrix is 4 cells by 4 cells.

7. Click **Generate Cells**.
   
   Tenable.sc displays the empty matrix for configuration.

8. Do one of the following:
   
   - **Edit a row or column header.**
     
     a. Click the header for the row or column you want to edit.
     
     b. Next to the header label, click the **menu**. The actions menu appears.
     
     c. Click **Edit Header**.
     
     d. In the **Label** box, type a new header.
     
     e. Click **Submit**.
   
   - **Add a matrix component.**
     
     a. Click the matrix cell where you want to add the component.
     
     b. In the **Data Type** drop-down box, select the type of data for the component.
     
     c. In the **Type** drop-down box, select the type of calculation you want the component to perform.
     
     d. In the **Source** drop-down box, select a data source.
     
     e. (Optional) In the **Filter** box, add or edit a filter using the same steps you would to add a filter to a report element; see [Manage Filter Components for a Single Element](#).
     
     f. In the **Rules** section, click **Add Rule** to add a rule.
Click the edit icon next to a rule to edit an existing rule.

g. Click **Submit** to save your changes to the component.

- **Copy a row or column.**
  
  a. Click the header for the row or column you want to copy.
  
  b. Next to the header label, click the 📊 menu.
  
  The actions menu appears.
  
  c. Click **Copy**.

  For columns, Tenable.sc inserts the copied column to the right of the original column.
  
  For rows, Tenable.sc inserts the copied row under the original row.

- **Delete a row or column.**
  
  a. Click the header for the row or column you want to delete.
  
  b. Next to the header label, click the 📊 menu.
  
  The actions menu appears.
  
  c. Click **Delete Cells**.

9. Click **Submit** to save your changes to the element.

10. Click **Submit** to save your changes to the report.

**Example**

<table>
<thead>
<tr>
<th>Current Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td><strong>New IP's</strong></td>
</tr>
<tr>
<td>&lt; 7 Days</td>
</tr>
<tr>
<td>8 - 14 Days</td>
</tr>
<tr>
<td>15 - 21 Days</td>
</tr>
<tr>
<td>22 - 30 Days</td>
</tr>
</tbody>
</table>
Configure a Table Element in a Report

**Required User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

A table element is a type of text element you can insert into a Tenable.sc report definition. For more information on text elements, see Configure a Text Element in a Report.

To configure a table element in a report:

1. Click **Reporting > Reports.**
   
   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.
   
   The **Edit Report** page appears.

3. In the left navigation bar, click **Definition.**
   
   The report outline appears. This outline is, by default, expanded. For more information, see Edit a Report Outline.

4. Do one of the following:

   - Add a new element.
     
     a. Click **Add Element.**
     
     b. In the **Text** section, click the **Table** icon.

   - Click the edit icon next to the element you want to change.

   **Tip:** To display Add Element and the edit icon next to an element, hover the cursor over the element.

5. Configure the **General** options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name for the element.</td>
</tr>
<tr>
<td>Location</td>
<td>Select a location for the element in the report.</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Style</td>
<td>Select a style for the element.</td>
</tr>
</tbody>
</table>

6. **Configure the Data options:**

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Equivalent to the <strong>Definition</strong> option of the same name in <strong>Report Options</strong>.</td>
</tr>
<tr>
<td>Query</td>
<td>Equivalent to the <strong>Definition</strong> option of the same name in <strong>Report Options</strong>.</td>
</tr>
<tr>
<td>Source</td>
<td>Equivalent to the <strong>Definition</strong> option of the same name in <strong>Report Options</strong>.</td>
</tr>
<tr>
<td>Tool</td>
<td>Equivalent to the <strong>Definition</strong> option of the same name in <strong>Report Options</strong>.</td>
</tr>
<tr>
<td>Filters</td>
<td>Equivalent to the <strong>Definition</strong> option of the same name in <strong>Report Options</strong>.</td>
</tr>
</tbody>
</table>

7. **Configure the Display options:**

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Results Displayed</td>
<td>Equivalent to the <strong>Display</strong> option of the same name in <strong>Report Options</strong>.</td>
</tr>
<tr>
<td>Sort Column</td>
<td>Equivalent to the <strong>Display</strong> option of the same name in <strong>Report Options</strong>.</td>
</tr>
<tr>
<td>Sort Direction</td>
<td>Equivalent to the <strong>Display</strong> option of the same name in <strong>Report Options</strong>.</td>
</tr>
<tr>
<td>Display Columns</td>
<td>Equivalent to the <strong>Display</strong> option of the same name in <strong>Report Options</strong>.</td>
</tr>
</tbody>
</table>

8. Click **Submit** to save your changes to the element.

9. Click **Submit** to save your changes to the report.

Example
## Highest Ranked Asset Vulnerability Index [Scan Result #23]

<table>
<thead>
<tr>
<th>Asset</th>
<th>Score</th>
<th>Total</th>
<th>Med.</th>
<th>High</th>
<th>Crit.</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Defined Assets</td>
<td>13593</td>
<td>1423</td>
<td>541</td>
<td>777</td>
<td>105</td>
</tr>
<tr>
<td>Linux Hosts</td>
<td>4185</td>
<td>476</td>
<td>193</td>
<td>237</td>
<td>26</td>
</tr>
<tr>
<td>Linux Kernel 2.6</td>
<td>4092</td>
<td>453</td>
<td>174</td>
<td>253</td>
<td>26</td>
</tr>
<tr>
<td>CentOS</td>
<td>3625</td>
<td>386</td>
<td>115</td>
<td>252</td>
<td>19</td>
</tr>
<tr>
<td>Linux Kernel 64-Bit</td>
<td>1294</td>
<td>144</td>
<td>68</td>
<td>61</td>
<td>12</td>
</tr>
<tr>
<td>Ubuntu Linux</td>
<td>380</td>
<td>48</td>
<td>40</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>Debian Linux</td>
<td>74</td>
<td>10</td>
<td>8</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Linux Kernel 3.1</td>
<td>9</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Linux Kernel 3.2</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Linux Kernel 3.3</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
# Configure a Charts Element in a Report

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

Charts elements in Tenable.sc reports include:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Relevant Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bar Chart</td>
<td><strong>Click to add a bar chart element to the report.</strong></td>
<td>PDF, RTF</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Bar Chart Example" /></td>
<td></td>
</tr>
<tr>
<td>Pie Chart</td>
<td><strong>Click to add a pie chart element to the report.</strong></td>
<td>PDF, RTF</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Pie Chart Example" /></td>
<td></td>
</tr>
<tr>
<td>Line Chart</td>
<td><strong>Click to add a line chart element to the report.</strong></td>
<td>PDF, RTF</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Line Chart Example" /></td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2020 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.
Line charts are defined by time (x-axis) and series data (y-axis). When selecting the time, available options include Relative time and Absolute time. One or more series data elements can be chosen and displayed as discrete lines for easy comparison.

Area charts are defined by time (x-axis) and series data (y-axis). When selecting the time, available options include Relative time and Absolute time. One or more series data elements can be chosen and displayed as a stackable view for easy comparison.

To configure a chart element in a report:

1. Click Reporting > Reports.
   
   The Reports page appears.

2. In the reports table, click the name of the report you want to edit.
   
   The Edit Report page appears.
3. In the left navigation bar, click **Definition**.

   The report outline appears. This outline is, by default, expanded. For more information, see **Edit a Report Outline**.

4. Do one of the following:

   - **Add a chart element**
     
     a. Click **Add Element** to add an element.
     
     b. In the **Charts** section, click the icon for the type of chart you want to add.

   - **Click the edit icon next to an existing chart element.**

   **Tip:** To display **Add Element** and the edit icon, hover the cursor over the element.

5. For all charts, configure the **General** options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name for the element.</td>
</tr>
<tr>
<td>Location</td>
<td>Select a location for the element in the report.</td>
</tr>
<tr>
<td>Style</td>
<td>Select a style for the element.</td>
</tr>
</tbody>
</table>

6. For bar charts and pie charts, configure the following **Data** options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Equivalent to the option the <strong>Definition</strong> option of the same name in <strong>Report Options</strong>.</td>
</tr>
<tr>
<td>Query</td>
<td>Equivalent to the option the <strong>Definition</strong> option of the same name in <strong>Report Options</strong>.</td>
</tr>
<tr>
<td>Source</td>
<td>Equivalent to the option the <strong>Definition</strong> option of the same name in <strong>Report Options</strong>.</td>
</tr>
<tr>
<td>Tool</td>
<td>Equivalent to the option the <strong>Definition</strong> option of the same name in <strong>Report Options</strong>.</td>
</tr>
</tbody>
</table>
7. For line charts and area charts, configure the following **Data** options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Type</td>
<td>Valid values are <strong>Relative</strong> and <strong>Absolute</strong>. Use to configure the x-axis of the chart.</td>
</tr>
<tr>
<td>Data Range</td>
<td>Use to configure the x-axis of the chart:</td>
</tr>
<tr>
<td></td>
<td>• If you select <strong>Relative</strong> for <strong>Data Type</strong>, select a relative date range.</td>
</tr>
<tr>
<td></td>
<td>• If you select <strong>Absolute</strong> for <strong>Data Type</strong>, select a specific start and end date for the data.</td>
</tr>
<tr>
<td>Series</td>
<td>Use to configure the y-axis of the chart. Line charts and area charts require that you configure at least one series.</td>
</tr>
</tbody>
</table>

8. For bar charts and pie charts, configure the following **Display** options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Results Displayed</td>
<td>Equivalent to the <strong>Display</strong> option of the same name in Report Options.</td>
</tr>
<tr>
<td>Sort Column</td>
<td>Equivalent to the <strong>Display</strong> option of the same name in Report Options.</td>
</tr>
<tr>
<td>Sort Direction</td>
<td>Equivalent to the <strong>Display</strong> option of the same name in Report Options.</td>
</tr>
<tr>
<td>Display Columns</td>
<td>Equivalent to the <strong>Display</strong> option of the same name in Report Options.</td>
</tr>
</tbody>
</table>

9. Click **Submit** to save your changes to the element.

10. Click **Submit** to save your changes to the report.
Reorder Report Chapters and Elements

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

In Tenable.sc, you can reorder chapters and elements in a PDF, CSV, or template-based report.

To reorder report chapters and elements:

1. Click **Reporting > Reports**.
   
The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.
   
The **Edit Report** page appears.

3. In the left navigation bar, click **Definition**.
   
The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).

4. Do one of the following:
   
   - In the report outline, click the report element, then drag and drop it to its new location.
   
   - Click the edit icon for the component, and select a new location in the **Location** dropdown box.

5. Click **Submit** to save your changes to the report.
Manage Filters for a Chapter Report

In Tenable.sc, PDF, RTF, and template-based reports use a chapter structure, so you can specify different filters for individual chapter elements of those reports.

You can manage filters for a single element or for multiple elements at the same time. For more information, see:

- Manage Filter Components for a Single Element
- Manage Filter Components for Multiple Elements
Manage Filter Components for a Single Element

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

**Tip:** You can build filters using one or more *filter components* with defined *filter component criteria*. Filter components are types of data (e.g., **CVE ID** or **Severity**). After you select a filter component, you specify the filter component criteria (e.g., a specific CVE ID or a specific severity level).

To manage filter components for a single element in a chapter report in Tenable.sc:

1. Click **Reporting > Reports**.
   
   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.
   
   The **Edit Report** page appears.

3. In the left navigation bar, click **Definition**.
   
   The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).

4. Click the edit icon next to the element you want to edit.

   **Tip:** To display icons next to a element, hover the cursor over the element.

5. Do one of the following:

   - **Add a filter component.**

     Use these steps to add one or more filter components to a single element. For information about the filter components available for vulnerability analysis data or event analysis data, see [Vulnerability Analysis Filter Components](#) or Event Analysis Filter Components.

     a. In the **Data** section, click **Add Filter**.

     b. Select a filter component from the drop-down box.

     c. Set the filter component criteria, as prompted.
Depending on the filter component you selected, Tenable.sc prompts you to type the value you want to filter for or to select from valid values and operators.

Note: If Tenable.sc does not prompt you to specify an operator, the unstated operator is equivalent to is equal to or is set to.

d. Click the check mark next to the filter component to stop editing it.

Note: The new filter component is not saved until you click Submit.

- Edit a filter component.
  a. In the Data section, click the edit icon next to the filter component.
  b. Edit the filter component criteria.
  c. Click the check mark next to the filter component to stop editing it.

Note: Your changes to the filter are not saved until you click Submit.

- Delete a filter component.

In the Data section, click the delete icon next to the filter component.

Note: Tenable.sc does not prompt you to confirm the deletion. However, the deletion is not final until you click Submit to save your changes.

6. Click Submit.
Manage Filter Components for Multiple Elements

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

When managing filter components for a chapter report in Tenable.sc, you can search the report for elements that use certain filter components, then update the filter component criteria for all matching elements in that report at the same time.

**Tip:** You can build filters using one or more *filter components* with defined *filter component criteria*. Filter components are types of data (e.g., **CVE ID** or **Severity**). After you select a filter component, you specify the filter component criteria (e.g., a specific CVE ID or a specific severity level).

You can use the following filter components to search and update: **Address**, **Audit File**, **Asset**, **CVE ID**, **DNS Name**, **IAVM ID**, **Repositories**, **Scan Policy**, and **Severity**.

For example, if you search a report definition for all elements where the **Severity** filter component is set to **Info**, you can update the **Severity** filter component to **Medium** for all elements, and add an **Audit File** filter component to the elements at the same time.

To manage filter components for multiple elements in a chapter report:

1. Click **Reporting > Reports**.
   
   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.
   
   The **Edit Report** page appears.

3. In the left navigation bar, click **Definition**.
   
   The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).

4. In the top navigation bar of the outline, click **Find/Update Filters**.

To search for specific elements in the report:

1. In the **Search Filters** section, click **Add Search Filter**.

2. Select a filter component from the drop-down box.
3. Select an operator from the drop-down box.
   a. If you selected **is equal to** or **contains** as operator, type filter component criteria or select a value from the list of valid filter component criteria, as appropriate to the filter component you selected.

4. Click the check mark at the end of the filter box.

   Tenable.sc searches the report outline for elements that match your search criteria and displays the results in the **Matching Filters** box.

**To specify the filter updates you want to make:**

1. In the **Update Actions** section, click **Add Search Filter**.
2. Select a filter component from the drop-down box.
3. Select an operator from the drop-down box.
4. Type filter component criteria or select a value from the list of valid filter values, as appropriate to the filter component and operator you selected.
5. Click the check mark at the end of the filter box.

**To review and update the filter updates:**

1. In the **Matching Filters** box, review the list to verify that you want to apply the update to all the listed elements.

   **Tip:** If you do not want to apply the current update to all the listed elements, it may be more appropriate to manage filter components by individual element. For more information, see [Manage Filter Components for a Single Element](#).

2. Click **Update Filters**.

   Tenable.sc applies the updates to the matching elements and returns you to the report outline.

3. Click **Submit** to save your changes to the report.
Manage Filter Components for a Non-Chapter Report

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

In Tenable.sc, CSV, DISA ARF, DISA ASR, and Cyberscope reports do not use a chapter structure, so you can create a set of filter components that apply to every element of the report.

**Tip:** You can build filters using one or more filter components with defined filter component criteria. Filter components are types of data (e.g., **CVE ID** or **Severity**). After you select a filter component, you specify the filter component criteria (e.g., a specific CVE ID or a specific severity level).

To manage filter components for a non-chapter report:

1. Click **Reporting** > **Reports**.
   
   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.
   
   The **Edit Report** page appears.

3. Do one of the following:

   - **Add a filter component.**

     Use these steps to add one or more filter components to a single element. For information about the filter components available for vulnerability analysis data or event analysis data, see [Vulnerability Analysis Filter Components](#) or Event Analysis Filter Components.

     a. In the **Definition** section, click **Add Filter**.

     b. Select a filter component from the drop-down box.

     c. Set the filter component criteria, as prompted.

        Depending on the filter component you selected, Tenable.sc prompts you to type the value you want to filter for or to select from valid values and operators.

     d. Click the check mark next to the filter component to stop editing it.

     **Note:** The new filter component is not saved until you click **Submit**.
• Edit a filter component.
  a. In the **Definition** section, click the edit icon next to the filter component.
  b. Edit the filter criteria.
  c. Click the check mark next to the filter component to stop editing it.

  **Note:** Your changes to the filter component are not saved until you click **Submit**.

• Delete a filter component.

  In the **Definition** section, click the delete icon next to the filter component.

  **Note:** Tenable.sc does not prompt you to confirm the deletion. However, the deletion is not final until you click **Submit** to save your changes.

4. Click **Submit** to save your changes.
View a Report Definition

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

To view a report definition:

1. Click **Reporting > Reports**.
   
The **Reports** page appears.

2. In the row for the report definition you want to view, click the menu.
   
The actions menu appears.

3. Click **View**.
   
   Tenable.sc displays a read-only version of the report definition.

**Note:** If you want to edit or delete the report definition from this page, see [Edit a Report Definition](#) or [Delete a Report Definition](#).
Copy a Report Definition

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

You can share a copy of a report definition with other users in your organization in Tenable.sc. This feature is useful for maintaining consistency throughout your organization.

After you share the copy, the other users own their local copy and can edit or delete as with any report they create themselves. Later changes you make to the original do not synchronize automatically to the copy.

To copy a report definition:

1. Click **Reporting > Reports**.
   
   The **Reports** page appears.

2. In the row for the report you want to copy, click the **menu**.
   
   The actions menu appears.

3. Click **Copy**.
   
   The **Copy Report** page appears.

4. In the **Group** box, select the group you want to grant access to a copy of the report.

5. Specify the user(s) that you want to grant access to a copy of the report.

6. Click **Copy**.
   
   Tenable.sc copies the report definition to the other accounts you specified. The copy retains its original title with "Copy of" prepended.
Export a Report Definition

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

In Tenable.sc, you can export a report definition as an XML file. This feature is useful for organizations running multiple Tenable.sc deployments to provide consistent reports without duplicating the work needed to create definition templates.

To export a report definition:

1. Click **Reporting > Reports**.
   
   The **Reports** page appears.

2. In the row for the definition you want to export, click the menu.

   The actions menu appears.

3. Click **Export**.

4. Do one of the following:

   - Click **Keep All References**.
     
     Object References are kept intact. Importing users should be within the same organization and have access to all relevant objects for the components to be useable.

   - Click **Remove All References**.
     
     All Object References are removed, altering the definitions of the components. Importing users do not need to make any changes for components to be useable.

   - Click **Replace with Placeholders**.
     
     Object References are removed and replaced with their respective names. Importing users can see the name of the reference object, but must replace it with an applicable object within their organization before the component is useable.

Tenable.sc downloads the report definition to your computer.
Import a Report Definition

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

In Tenable.sc, you can only import XML files in the same format used to export report definitions. This feature is useful for organizations running multiple Tenable.sc deployments to provide consistent reports without duplicating the work needed to create definition templates.

To import a report definition:

1. Copy the report definition file to your local computer.
2. Click **Reporting > Reports**.
   
The **Reports** page appears.
3. In the top right corner of the page, click **Options**.
4. Click **Import Report**.
5. In the **Name** box, type a name for the report.
6. Click **Choose File** next to the **Report Definition** box.
7. Browse to the local copy of the report definition XML file.
8. Click **Import**.
   
   Tenable.sc imports the report definition.
9. (Optional) Click **Edit the report definition** as desired.
Delete a Report Definition

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

To delete a report definition:

1. Click **Reporting > Reports**.
   
   The **Reports** page appears.

2. In the row for the report you want to delete, click the 🌐 menu.
   
   The actions menu appears.

3. Click **Delete**.

4. Click **Delete** to confirm the deletion.

   Tenable.sc deletes the report definition.

**Note:** Tenable.sc retains any report results associated with the deleted definition. You must manually delete results associated with the report.
Launch a Report on Demand

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

To launch a report on demand:

1. Click **Reporting > Reports**.
   
   The **Reports** page appears.
2. Click the gray triangle icon next to the report you want to launch.
   
   Tenable.sc starts the report.
3. (Optional) Monitor the status of the report in the **Report Results** page.
   
   To view this page, do one of the following:

   - Click **View Report Results** in the launch notification message.
   - Click **Reporting > Report Results** in the top navigation bar.

**Note:** In the **Report Results** page, you can also stop the currently running report.
Manage Report Results

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

On the [Report Results](#) page of Tenable.sc, you can manage both currently running reports and completed report results. Completed report results include successful and failed report runs, so you can access and distribute a successful report result or troubleshoot a report failure.

To manage report results:

1. Click **Reporting > Report Results**.
   
The Report Results page appears.

2. You can:
   - [Filter existing report results in the report results table](#).
   - [Stop a currently running report](#).
   - [Download a successful report result to your computer](#).
   - [View a successful report result](#).
   - [Publish a successful result](#).
   - [Email a copy of a successful result to specified users](#).
   - [Share a copy of a successful result with other Tenable.sc user accounts](#).
   - [View error conditions for a failed report](#).
   - [Delete a report result](#).
Stop a Running Report

Required User Role: Organizational user with appropriate permissions. For more information, see User Roles.

If you want to stop a report that is currently running:

1. Click Reporting > Report Results.
   The Report Results page appears.

2. Click the gray square icon next to the report you want to stop.
   Tenable.sc stops the report run.

   **Note:** You cannot restart a stopped report run. You can only launch the report again.
Download a Report Result

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

To download a successful report result to your computer:

1. Click **Reporting > Report Results**.
   
   The **Report Results** page appears.

2. Do one of the following:
   
   - In the Results table, click the name of the report.
   - Click the download icon next to the report result in the results table.
   - Click the ⚙ menu next to the report result.

   The actions menu appears.

   a. Click **Download**.
View a Report Result

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

To view a successful report result:

1. Click **Reporting > Report Results**.
   
The Report Results page appears.

2. In the row for the report result you want to view, click the menu.
   
The actions menu appears.

3. Click **View**.
   
The report appears.

4. (Optional) To download the report result to your computer, click **Download**.

5. (Optional) To delete the report result, click **Delete**.
Publish a Report Result

**Required User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

To publish a successful report result:

1. Click **Reporting > Report Results**.
   
   The **Report Results** page appears.

2. In the row for the report result you want to publish, click the ☰ menu.
   
   The actions menu appears.

3. Click **Publish**.
   
   The **Publish Report Results** window appears.

4. Search for and select a publishing site.

5. Click **Publish**.
Email a Report Result

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

To email a copy of a successful report result to specific users:

1. Click **Reporting > Report Results.**
   
   The **Report Results** page appears.

2. In the row for the report result you want to email, click the ![icon] menu.
   
   The actions menu appears.

3. Click **Email.**

4. Do one of the following:
   
   - Use the **Group** and **User** boxes to select the Tenable.sc user or users you want to receive the report result.
   
   - Type the email address of recipients who are not Tenable.sc users.

5. Click **Submit.**
Copy a Report Result

Required User Role: Organizational user with appropriate permissions. For more information, see User Roles.

To share a copy of a successful result with other Tenable.sc user accounts:

1. Click Reporting > Report Results.
   
   The Report Results page appears.

2. In the row for the report result you want to copy, click the ⚙ menu.
   
   The actions menu appears.

3. Click Copy.

4. In the Group box, select the group you want to grant access to a copy of the report result.

5. Specify a user or users that you want to grant access to a copy of the report result.

6. Click Copy.

   Tenable.sc copies the report result to the other accounts you specified. The copy retains its original title with "Copy of" prepended.
View Errors for a Failed Report

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

To view error conditions for a failed report:

1. Click **Reporting > Report Results**.
   
The **Report Results** page appears.

2. Click the name of the failed result in the results table.
   
The **View Report Results** page appears.

3. Review the **Error Details** section.
Delete a Report Result

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

To delete a report result:

1. Click **Reporting > Report Results**.  
   The **Report Results** page appears.
2. In the row for the result you want to delete, click the menu.  
   The actions menu appears.
3. Click **Delete**.
4. Click **Delete** to confirm the deletion.
CyberScope and DISA Report Attributes

Report attributes are used for adding required information to CyberScope or DISA report types. After you create an attribute, you can select it during CyberScope, DISA ARF, or DISA Consolidated ARF report creation. For more information, see Create a Custom Report.

To filter the Report Attributes page, see Apply a Filter.

Configure the following options, including options specific for your attribute type: CyberScope Options or DISA Options.

<table>
<thead>
<tr>
<th>General Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the attribute.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) A description for the attribute.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of attribute you want to create. Your Type selection determines the other options you must configure: CyberScope Options or DISA Options.</td>
</tr>
</tbody>
</table>

CyberScope Options

The following table describes the additional options to configure when configuring a CyberScope attribute.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting Component</td>
<td>The CyberScope value for a reporting component (e.g., Department of Justice).</td>
</tr>
<tr>
<td>Component Bureau</td>
<td>The CyberScope value for a FISMA reporting entity within the Reporting Component (e.g., Justice Management Division).</td>
</tr>
<tr>
<td>Enclaves</td>
<td>The CyberScope value for an enclave associated with the Reporting Component or Component Bureau.</td>
</tr>
</tbody>
</table>

DISA Options

The following table describes the additional options to configure when configuring a DISA attribute.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Owning Unit</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>(Required) The Cyber Operational Attributes Management System (COAMS) fully qualified hierarchy name of the owning organization.</td>
</tr>
<tr>
<td><strong>Owning Service</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>The COAMS fully qualified hierarchy name of the owning combatant command, service, or agency.</td>
</tr>
<tr>
<td><strong>Current AOR</strong></td>
<td>The COAMS fully qualified hierarchy name of the appropriate combatant command area of responsibility (COCOM AOR).</td>
</tr>
<tr>
<td><strong>Region</strong></td>
<td>A region for the owning service.</td>
</tr>
<tr>
<td><strong>Administration Unit</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>The COAMS fully qualified hierarchy name of the administering organization.</td>
</tr>
<tr>
<td><strong>Administration POC</strong></td>
<td>Any required information you need to provide about the administration unit's point of contact (POC).</td>
</tr>
<tr>
<td><strong>Tip:</strong></td>
<td>Tenable recommends leaving the Generational Qualifier option blank.</td>
</tr>
<tr>
<td><strong>CND Service Provider</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>The COAMS fully qualified hierarchy name of the Computer Network Defense Service Provider (CNDSP).</td>
</tr>
<tr>
<td><strong>Por Managed</strong></td>
<td>(Required) Specifies if the reported assets are centrally managed by a program management office (PMO): true or false.</td>
</tr>
<tr>
<td><strong>System Affiliation</strong></td>
<td>The COAMS operationalacredit value that specifies the fully qualified hierarchy name of the system affiliation.</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Tip:</strong></td>
<td>Tenable recommends leaving all options blank except the Street Address. The Street Address</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>specifies the COAMS geolocation area.</td>
</tr>
</tbody>
</table>
Report Images

**Note:** Image files must be of type .png or .jpg. Images used must be consistent when selecting the bit depth (8-bit, 16-bit, 24-bit, etc.). Otherwise, errors might be encountered when generating reports.

In Tenable.sc, the **Report Images** interface allows a user with permissions to view details, add, edit, or delete PDF report images. From this interface, you can manage two types of images: logos and watermarks. Logos appear at the bottom of each page, while watermarks appear prominently across the center of the report page.

To filter the Report Images page, see [Apply a Filter](#).

**Report Image Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Add     | Add a new logo or watermark image. Note that only PNG and JPEG formats are supported. The default image sizes are as follows, all at 300 DPI:  
  - default-cover-logo = 987x130  
  - default-footer-logo = 380x100  
  - default-page-logo = 579x84 |
<table>
<thead>
<tr>
<th><strong>Option</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>default-watermark = 887x610</td>
<td>While there are no set limitations on image size or resolution, using images that are different from these specifications can have a negative impact on report appearance.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The image size must be set to 300 DPI to prevent image breaks.</td>
</tr>
<tr>
<td>Edit</td>
<td>Edit any of the selected image’s options, including name, description, type and file.</td>
</tr>
<tr>
<td>Detail</td>
<td>View image details including: name, description, date uploaded, last modified and type.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete the highlighted image.</td>
</tr>
</tbody>
</table>
Filters

You can apply filters on many pages of the Tenable.sc Director web interface to filter the data displayed on the page. After you build and apply a filter, the number next to the filter icon (ictionaries) updates to indicate the number of filters currently applied to the list.

You can build filters using one or more filter components with defined filter component criteria. Filter components are types of data (e.g., CVE ID or Severity). After you select a filter component, you specify the filter component criteria (e.g., a specific CVE ID or a specific severity level).

For more information, see Apply a Filter and Vulnerability Analysis Filter Components.

If you want to save a filter for repeated use, create a query, as described in Queries.
Apply a Filter

**Required User Role:** Any

You can use filters to narrow the data displayed on specific pages in the Tenable.sc Director web interface. Some pages expand the filter options in the left side bar and some expand the filter options in the right side bar.

For more information, see [Filters](#).

To filter data on a Tenable.sc Director page with a left side bar:

1. Log in to Tenable.sc Director via the user interface.
2. Navigate to any page that supports filtering.
3. On the left side of the page, click the double arrow (»).
   
   The **Filters** side bar expands.

4. Click **Select Filters**.
   
   The filter components selection window appears.
For more information about the components supported for your analysis view, see Vulnerability Analysis Filter Components.

5. Select one or more filter component check boxes.

6. Click Apply.

The Filters side bar updates to show the filter components you selected.

7. Click the box for the filter component.

The filter component criteria selection window appears.
8. Modify the filter component criteria.

9. Click **OK**.

The **Filters** side bar updates to show the filter component criteria you modified. The **Apply All** button appears.

10. Click **Apply All**.

The page updates to reflect the filter you applied.

To filter data on a Tenable.sc Director page with an inline filter icon and right side bar:
1. Log in to Tenable.sc Director via the user interface.

2. Navigate to any page that supports filtering.

3. Locate the filter icon (filter icon).

The **Filters** side bar expands.

4. Click the box for a filter component.

   The filter component criteria selection window appears.
For more information about the components supported for your analysis view, see Vulnerability Analysis Filter Components.

5. Modify the filter component criteria.

6. Click Apply.

The Filters side bar updates to show the filter component criteria you modified. The page updates to reflect the filter you applied.
Queries

The Queries page displays a list of queries available for use. The information provided includes Name, Type, Group, Owner, and the Last Modified time. You can use a filter to narrow the list by any of the columns (except Last Modified). For more information, see Filters.

To add a query, see Add or Save a Query. To load a query, see Load a Query.

Click on the Query Name to display an edit page and modify the selected query.

Query Options

Queries provide the ability to save custom views of vulnerability, event, ticket, user, and alert data for repeated access.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the query.</td>
</tr>
<tr>
<td>Description</td>
<td>A description for the query.</td>
</tr>
<tr>
<td>Tag</td>
<td>A tag for the query. For more information, see Tags.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of data you want the query to use. For more information about the filter components for Vulnerability, Event, and Mobile data types, see Vulnerability Analysis Filter Components, Event Analysis Filter Components, and Mobile Analysis. For more information about the filter components for Ticket, User, and Alert data types, see Ticket-Specific Query Options, User-Specific Query Options, and Alert-Specific Query Options.</td>
</tr>
<tr>
<td>Tool</td>
<td>Chooses the analysis tool used by the query.</td>
</tr>
</tbody>
</table>

Ticket-Specific Query Options

Ticket queries are a useful way of determining what tickets to alert against. For example, if you want to be alerted when a user named Joe is assigned a ticket, you could create a query with a ticket filter based on the Assignee value of Joe. You could then create an alert to email you when Joe was assigned a ticket. The table below contains a list of the ticket query options.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Ticket name to filter against</td>
</tr>
<tr>
<td>Status</td>
<td>Ticket status to filter against.</td>
</tr>
<tr>
<td>Classification</td>
<td>The ticket classification to filter against.</td>
</tr>
<tr>
<td>Owner</td>
<td>The manager (owner) of the ticket assignee.</td>
</tr>
<tr>
<td>Assignee</td>
<td>The ticket assignee to filter against.</td>
</tr>
<tr>
<td>Created Timeframe</td>
<td>Ticket creation date/time to filter against. Either specify an explicit</td>
</tr>
<tr>
<td></td>
<td>timeframe, including the start and end time or choose one of the predefined</td>
</tr>
<tr>
<td></td>
<td>periods (e.g., last 15 minutes, last hour, etc.)</td>
</tr>
<tr>
<td>Assigned Timeframe</td>
<td>Ticket assigned date/time to filter against. Either specify an explicit</td>
</tr>
<tr>
<td></td>
<td>timeframe, including the start and end time or choose one of the predefined</td>
</tr>
<tr>
<td></td>
<td>periods (e.g., last 15 minutes, last hour, etc.)</td>
</tr>
<tr>
<td>Modified Timeframe</td>
<td>Ticket modified date/time to filter against. Either specify an explicit</td>
</tr>
<tr>
<td></td>
<td>timeframe, including the start and end time or choose one of the predefined</td>
</tr>
<tr>
<td></td>
<td>periods (e.g., last 15 minutes, last hour, etc.)</td>
</tr>
<tr>
<td>Resolved Timeframe</td>
<td>Ticket resolution date/time to filter against. Either specify an explicit</td>
</tr>
<tr>
<td></td>
<td>timeframe, including the start and end time or choose one of the predefined</td>
</tr>
<tr>
<td></td>
<td>periods (e.g., last 15 minutes, last hour, etc.)</td>
</tr>
<tr>
<td>Closed Timeframe</td>
<td>Ticket closed date/time to filter against. Either specify an explicit</td>
</tr>
<tr>
<td></td>
<td>timeframe, including the start and end time or choose one of the predefined</td>
</tr>
<tr>
<td></td>
<td>periods (e.g., last 15 minutes, last hour, etc.)</td>
</tr>
</tbody>
</table>

### User-Specific Query Options

User queries are useful for reporting, dashboards and alerts based on user actions. For example, they can track user logins and locked accounts. They can also track user logins from accounts not authorized on the monitored systems.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>User first name to filter against.</td>
</tr>
<tr>
<td>Last Name</td>
<td>User last name to filter against.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Username</td>
<td>Actual username to filter against.</td>
</tr>
<tr>
<td>Group</td>
<td>Filter against the group the user(s) belong to.</td>
</tr>
<tr>
<td>Role</td>
<td>Filters against users who have the specified role.</td>
</tr>
<tr>
<td>Email</td>
<td>Filters against users based on their email address.</td>
</tr>
<tr>
<td>Last Login Timeframe</td>
<td>Filters against users whose last login was that the timeframe specified. Either specify an explicit timeframe, including the start and end time or choose one of the predefined periods (e.g., last 15 minutes, last hour, etc.).</td>
</tr>
<tr>
<td>Account State</td>
<td>Filters against the user account state (locked vs. unlocked).</td>
</tr>
</tbody>
</table>

**Alert-Specific Query Options**

The Alert query is useful for reporting, dashboards and alerting when an alert has triggered. This is useful for situations where a report, dashboard element or conditional alert is required after the specified alert filter conditions have been met. For example, a daily report could be scheduled containing a query of all active alerts and their details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Filter against alerts with the specified name.</td>
</tr>
<tr>
<td>Description</td>
<td>Filter against alerts with the specified description.</td>
</tr>
<tr>
<td>State</td>
<td>Choose from <strong>All</strong>, <strong>Triggered</strong>, or <strong>Not Triggered</strong>.</td>
</tr>
<tr>
<td>Created Timeframe</td>
<td>Filters against the alert creation timeframe specified. Either specify an explicit timeframe, including the start and end time or choose one of the predefined periods (e.g., last 15 minutes, last hour, etc.).</td>
</tr>
<tr>
<td>Modified Timeframe</td>
<td>Filters against the most recent alert modification timeframe specified. Either specify an explicit timeframe, including the start and end time or choose one of the predefined periods (e.g., last 15 minutes, last hour, etc.).</td>
</tr>
<tr>
<td>Last Triggered Timeframe</td>
<td>Filters against the most recent alert trigger timeframe specified. Either specify an explicit timeframe, including the start and end time or choose one of the predefined periods (e.g., last 15 minutes, last hour, etc.).</td>
</tr>
<tr>
<td>Last Evaluated Timeframe</td>
<td>Filters against the most recent alert evaluation timeframe specified. Either specify</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ated Time-frame</td>
<td>an explicit timeframe, including the start and end time or choose one of the pre-defined periods (e.g., last 15 minutes, last hour, etc.).</td>
</tr>
</tbody>
</table>
Add or Save a Query

**Required User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can add queries from the Queries page or from the Vulnerability Analysis page, Event Analysis page, or Mobile Analysis page. For more information about query options, see Queries.

**Note:** If you want to create a mitigated vulnerabilities query, you must add the query from the Vulnerability Analysis page.

To add a query from the Queries page:

1. Log in to Tenable.sc via the user interface.
2. Click Analysis > Queries.
   
The Queries page appears.
3. Click Add.
4. Type a Name and Description.
5. (Optional) If you want to add a tag, type select a Tag from the drop-down. For more information, see Tags.
6. Select a Type.
   
The Tool drop-down updates with options for that type.
7. Select a Tool.
8. Click Add Filter.
   
The Filters section expands. For more information, see Filters.
9. Select a filter component from the Select a Filter drop-down.
   
The filter component criteria box appears.
10. In the filter component criteria box, type or select filter component criteria.
11. Click the apply icon (✔).
   The filter component is added.
12. (Optional) To add other filter components, repeat step 8.
13. Click **Submit**.
   Tenable.sc Director saves your configuration.

To save a query from an analysis page:
1. Log in to Tenable.sc via the user interface.
2. Click **Analysis > Vulnerabilities, Analysis > Events**, or **Analysis > Mobile**.
   The analysis page appears.
3. Apply a filter for the query, as described in [Apply a Filter](#).
   The page updates to reflect the filter you applied.
4. In the **Options** drop-down box, click **Save Query**.
5. In the **Name** box, type a name for the query.
6. In the **Description** box, type a description for the query.
7. (Optional) If you want to add a tag, type or select a **Tag** from the drop-down. For more information, see [Tags](#).
8. Click **Submit**.
   Tenable.sc Director saves your configuration.
Load a Query

**Required User Role:** Any

You can load queries from any page that supports filtering.

To load a query:

1. Log in to Tenable.sc Director via the user interface.
2. Navigate to any page that supports filtering.
3. On the left side of the page, click the double arrow ( »).
   - The **Filters** side bar expands.
4. Click **Load Query**.
5. Select the query you want to load.
6. Click **Apply**.
   - The page updates, filtered by the query you selected.
Workflow Actions

Workflow actions allow organizational users to configure and manage alerting and ticketing. These functions allow the user to be notified of and properly handle vulnerabilities and events as they come in.

For more information, see Alerts and Tickets.
Alerts

Path: **Workflow > Alerts**

Tenable.sc Director can be configured to perform actions, such as email alerts, for select vulnerability or alert occurrences to various users regardless of whether the events correlate to a local vulnerability or not. Other alert actions include UI notification, ticket creation/assignment, remediation scans, launching a report, email notification, and syslog alerting. Many actions can be assigned per ticket.

Click the **menu** to add an Alert from the main Alerts page. Here you can, **Edit, Evaluate, View** (view details of), and **Delete** alerts. The **Evaluate** option allows an alert to be tested whether it has met the configured time criteria or not. Clicking on an alert will take the user to the Edit Alert page for the selected alert.

<table>
<thead>
<tr>
<th>Alert Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Alert name</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive text for the alert</td>
</tr>
<tr>
<td>Schedule</td>
<td>The setting will determine how often the alert checks for the conditions to be matched. Selections vary in frequency from 15 minutes to monthly. Selecting the option of Never will create the alert to be launched only on demand.</td>
</tr>
<tr>
<td>Behavior</td>
<td>If set to alert on the first occurrence, the alert will only trigger when the condition initially changes from false to true. The other option is to trigger on each detection of the true condition.</td>
</tr>
<tr>
<td>Type</td>
<td><strong>Vulnerability, Event, or Ticket.</strong></td>
</tr>
<tr>
<td>Trigger</td>
<td></td>
</tr>
</tbody>
</table>
|              | - **IP Count** – Trigger on vulnerabilities or events whose IP address count matches the given parameters.  
|              | - **Unique Vulnerability/Event Count** – Trigger an alert when the vulnerability/event count matches the given parameters. This option is set to **Unique Vulnerability Count** for vulnerability alerts and **Event Count** for event alerts.  
<p>|              | - <strong>Port Count</strong> – Trigger an alert when the events/vulnerabilities using a certain port number match the given parameters. |</p>
<table>
<thead>
<tr>
<th>Alert Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query</td>
<td>The dataset to which the trigger condition will be compared.</td>
</tr>
</tbody>
</table>
| Filters      | Apply advanced filters to the vulnerability or event data. The complete filter set may be created here, or if a Query was selected those parameters may be edited.  
For more information, see [Filters](#). |
| Add Actions  | Adding actions will determine what the alert does with triggered events. The options are **Assign Ticket**, **Email**, **Generate Syslog**, **Launch Scan**, **Launch Report**, or **Notify Users**. Multiple actions may be triggered for each alert.  
For more information, see [Alert Actions](#). |

### Alert Actions

**Tip:** Use email alerts to interface with third-party ticketing systems by adding variables in the message option.

<table>
<thead>
<tr>
<th>Action Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Subject line of the alert email.</td>
</tr>
</tbody>
</table>
| Message       | Message of the alert email. Within the message body, the following variables can be defined for email message customization:  
- **Alert ID** – Designated with the variable: `%alertID%`, this specifies the unique identification number assigned to the alert by Tenable.sc Director.  
- **Alert name** – Designated with the variable: `%alertName%`, this specifies the name assigned to the alert (e.g., “Test email alert”).  
- **Trigger Name** – Designated with the variable: `%triggerName%`, this specifies if the trigger is IP address count, Vulnerability count, or Port count.  
- **Trigger Operator** – Designated with the variable: `%triggerOperator%`, this specifies which operator was used for the count: `>=, =, >=` or `!=`. |
<table>
<thead>
<tr>
<th>Action Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trigger value</strong> – Designated with the variable: %triggerValue%, this specifies the specific threshold value set that will trigger the alert.</td>
<td></td>
</tr>
<tr>
<td><strong>Calculated value</strong> – Designated with the variable: %calculatedValue%, this specifies the actual value that triggered the alert.</td>
<td></td>
</tr>
<tr>
<td><strong>Alert Name</strong> – Designated with the variable: %alertName%, this specifies the name given to the alert within Tenable.sc Director.</td>
<td></td>
</tr>
<tr>
<td><strong>Alert owner</strong> – Designated with the variable: %owner%, this specifies the user that created the alert.</td>
<td></td>
</tr>
<tr>
<td><strong>SC URL</strong> – Designated with the variable: %url%, this specifies the URL that the Tenable.sc Director can be accessed with. This is useful where the URL that users can access Tenable.sc Director with differs from the URL known by Tenable.sc Director.</td>
<td></td>
</tr>
</tbody>
</table>

The sample email alert below contains some of these keywords embedded into an HTML email:

Alert `<strong>%alertName%</strong>` (id #%alertID%) has triggered.

`<strong>Alert Definition:</strong> %triggerName% %triggerOperator% %triggerValue%

`<strong>Calculated Value:</strong> %calculatedValue%

Please visit your Tenable.sc Director (`<a href- f="%url%">%url%</a>`) for more information.

This e-mail was automatically generated by Tenable.sc Director as a result of alert `<strong>%alertName%</strong>` owned by `<strong>%owner%</strong>`. 
<table>
<thead>
<tr>
<th><strong>Action Option</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Include Results</strong></td>
<td>If this box is checked, the query results (maximum of 500) that triggered the alert are included in the email.</td>
</tr>
<tr>
<td><strong>Users</strong></td>
<td>Users who will be emailed. The user email address is used with this function.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If a user is configured within the email action and that user is deleted, the action option within the alert turns red. In addition, a notification is displayed for the new alert owner with the new alert status. To resolve this, edit the alert action definitions and choose “Edit Action” to apply the correct user(s).</td>
</tr>
<tr>
<td><strong>Email Addresses</strong></td>
<td>Additional email addresses to send the alert to. For multiple recipients, add one email address per line or use a comma-separated list.</td>
</tr>
<tr>
<td><strong>Notify Users</strong></td>
<td><strong>Message</strong> Custom notification message to generate when the alert triggers.</td>
</tr>
<tr>
<td><strong>Users</strong></td>
<td>Users who will receive the notification message.</td>
</tr>
<tr>
<td><strong>Generate Syslog</strong></td>
<td><strong>Host</strong> Host that will receive the syslog alert.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>UDP port used by the remote syslog server.</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Severity level of the syslog messages (<strong>Critical</strong>, <strong>Warning</strong>, or <strong>Notice</strong>).</td>
</tr>
<tr>
<td><strong>Message</strong></td>
<td>Message to include within the syslog alert.</td>
</tr>
<tr>
<td><strong>Assign Ticket</strong></td>
<td><strong>Name</strong> Name assigned to the ticket</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Ticket description</td>
</tr>
<tr>
<td><strong>Assignee</strong></td>
<td>User who will receive the ticket</td>
</tr>
<tr>
<td>Action Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Scan</td>
<td>Scan template to be used for the alert scan. Allows the user to select from a list of available scan templates to launch a scan against a triggered host.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The scanned host will be the host that triggered the scan and not the host within the scan template itself. IPs used for the scan targets are limited to the top 100 results of the alert query.</td>
</tr>
<tr>
<td>Report</td>
<td>Allows the user to select an existing report template and generate the report based on triggered alert data.</td>
</tr>
</tbody>
</table>
Tickets

Tickets can be created both manually and automatically by a predefined set of conditions through the alerting functionality described above.

For more information, see [Open a Ticket](#).

<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>Name assigned to the ticket.</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive text for the ticket.</td>
</tr>
<tr>
<td>Notes</td>
<td>Notes for the ticket assignee.</td>
</tr>
<tr>
<td>Assignee</td>
<td>User that the ticket is assigned to.</td>
</tr>
</tbody>
</table>

**Note:** If the ticket assignee is deleted, the ticket is automatically reassigned to the assignee’s owner along with a notification message indicating that the ticket has been reassigned.

<table>
<thead>
<tr>
<th>Status (Available during edit)</th>
<th>The following ticket statuses become available after a ticket has been created and are available from the Edit page:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Assigned&lt;br&gt;• Resolved&lt;br&gt;• More Information&lt;br&gt;• Not Applicable&lt;br&gt;• Duplicate&lt;br&gt;• Closed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Classification</th>
<th>Ticket classification can be selected from a drop-down box containing such items as Information, Configuration, Patch, Disable, False Positive, and many others.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Vulnerability, Event, or Ticket.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a Query</td>
<td>List of queries to choose from for the ticket assignee to help provide context for coming up with a resolution.</td>
</tr>
</tbody>
</table>
In addition to adding and editing tickets, a **Browse** command button is available. This option enables the user to view the vulnerability snapshot added during ticket creation. The displayed view matches the query that was used by the ticket.

To view details about an existing ticket, click the ticket to bring up the edit ticket page, use the **Edit** option from the menu to view options that were set during the **Add Ticket** process or use the **View** option from the menu to view a Ticket Detail summary with the name, status, creator, assignee, history, queries, description, and ticket notes.

Once a ticket has been mitigated, click **Resolve** from the menu to provide ticket resolution.

Once the ticket is resolved it may be closed from the **Close** option from the menu.

Within the **Status** drop-down box, the user can select from one of these status options: Assigned, Resolved, More Information, Duplicate, or Not Applicable. Choose the correct status and add notes relevant to the ticket resolution. Resolved tickets still show up in the user’s ticket queue with an **Active** status. Closing a ticket removes the ticket from the **Active** status filter view, but does not provide the ability to add notes similar to the **Update Ticket** function. Tickets in the **Resolved** or **Closed** state can always be reopened as needed.
Open a Ticket

**Required User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

You can use tickets within Tenable.sc Director to coordinate the assessment and remediation of vulnerabilities and security events.

You can configure a ticket from an analysis page, or from the Tickets page. For more information about the options to configure, see [Tickets](#).

To open a ticket from an analysis page:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Analysis > Vulnerabilities**.
   
   The **Vulnerability Analysis** appears.
3. In the upper-right corner, click the **Options** drop-down box.
4. Click **Open Ticket**.
5. In the **Name** box, type a name.
6. (Optional) In the **Description** box, type a description.
7. (Optional) In the **Notes** box, type a note to the assignee.
8. In the **Assignee** drop-down box, select an assignee.
9. In the **Classification** drop-down box, select a classification.
10. Click **Submit**.
    
    Tenable.sc Director creates the ticket.

To open a ticket from the Tickets page:

1. Log in to Tenable.sc Director via the user interface.
2. Click **Workflow > Tickets**.
   
   The **Tickets** page appears.
3. Click **Add**.
4. In the **Name** box, type a name.

5. (Optional) In the **Description** box, type a description.

6. (Optional) In the **Notes** box, type a note to the assignee.

7. In the **Assignee** drop-down box, select an assignee.

8. In the **Classification** drop-down box, select a classification.

9. (Optional) Click **Add Query View**.

10. Click **Submit**.

    Tenable.sc Director creates the ticket.
Additional Resources

The topics in this section offer guidance in areas related to Tenable.sc Director.

- Start, Stop, or Restart Tenable.sc Director
- License Declarations
- Encryption Strength
- Perform an Offline Tenable.sc Director Plugin/Feed Updates
- Troubleshooting
Start, Stop, or Restart Tenable.sc Director

**Required User Role:** Root user

When Tenable.sc is installed, the required services are started by default.

To change the status of Tenable.sc Director:

1. Log in to Tenable.sc Director via the CLI.
2. Run the following command to check the status of your Tenable.sc Director:
   ```
   # service SecurityCenter status
   ```
   The system indicates whether Tenable.sc Director is running or stopped.
3. Run one of the following commands to change the status of your Tenable.sc Director:
   - To start Tenable.sc Director, run:
     ```
     # service SecurityCenter start
     ```
   - To stop Tenable.sc Director, run:
     ```
     # service SecurityCenter stop
     ```
   - To restart Tenable.sc Director, run:
     ```
     # service SecurityCenter restart
     ```
License Declarations

Tenable.sc Director’s Software License Agreement can be found on Tenable.sc Director in the /opt/sc/docs directory.

For a list of third-party software packages that Tenable utilizes with Tenable.sc Director, see Tenable Third-Party License Declarations.
## Encryption Strength

Tenable.sc Director uses the following default encryption for storage and communications.

<table>
<thead>
<tr>
<th>Function</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storing TNS user account passwords</td>
<td>SHA-512 and the PBKDF2 function</td>
</tr>
<tr>
<td>Storing user and service accounts for scan credentials, as described in Credentials.</td>
<td>AES-256-CBC</td>
</tr>
<tr>
<td>Storing scan data, as described in Repositories.</td>
<td>None</td>
</tr>
<tr>
<td>Communications between Tenable.sc and clients (Tenable.sc users).</td>
<td>SSL/TLS 1.2 with the strongest encryption method supported by Tenable.sc Apache and your browser, CLI program, or API program: ECDHE+AESGCM, EDH+AESGCM, AES256+EECDH, or AES256+EDH. For more information about strong encryption, see Configure SSL/TLS Strong Encryption.</td>
</tr>
<tr>
<td>Communications between Tenable.sc and the Tenable product registration server.</td>
<td>SSL/TLS 1.2 with ECDHE-RSA-AES256-GCM-SHA384</td>
</tr>
<tr>
<td>Communications between Tenable.sc and the Tenable plugin update server.</td>
<td>SSL/TLS 1.2 with ECDHE-RSA-AES256-GCM-SHA384</td>
</tr>
<tr>
<td>Communications between Tenable.sc and:</td>
<td></td>
</tr>
<tr>
<td>• Nessus or Nessus or Nessus</td>
<td>SSL/TLS 1.2 with the strongest encryption method supported by Tenable.sc Apache and your browser, CLI program, or API program: ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-SHA384, or ECDHE-RSA-AES256-GCM-SHA384.</td>
</tr>
<tr>
<td>Function</td>
<td>Encryption</td>
</tr>
<tr>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>sus Manager</td>
<td></td>
</tr>
<tr>
<td>• Tenable.io</td>
<td></td>
</tr>
<tr>
<td>• NNM</td>
<td></td>
</tr>
<tr>
<td>• LCE</td>
<td></td>
</tr>
<tr>
<td>Synchronizations between Tenable.sc and Tenable.io for Lumin.</td>
<td>SSL/TLS 1.2</td>
</tr>
</tbody>
</table>
Configure SSL/TLS Strong Encryption

You can configure SSL/TLS strong encryption for Tenable.sc Director-client communications to meet the security needs of your organization. For more information about Tenable.sc encryption, see Encryption Strength.

To configure SSL/TLS strong encryptions for Tenable.sc Director communications:

1. Open the /opt/sc/support/conf/sslciphers.conf file in a text editor.
2. Add the following content at the end of the file:

   ```plaintext
   SSLCipherSuite <cipher you want to use for SSL/TLS encryption>
   ```

   For example:

   ```plaintext
   # SSL Ciphers
   SSLProtocol ALL -SSLv2 -SSLv3
   SSLHonorCipherOrder On
   SSLCompression off
   ```

3. Restart Tenable.sc Director, as described in Start, Stop, or Restart Tenable.sc Director. Tenable.sc Director restarts.

4. In /opt/sc/support/logs, open ssl_request_log.

    The log file text appears.

5. Verify the configuration in ssl_request_log matches the cipher you specified. If the configuration and cipher do not match, investigate the following:

   - Confirm that you provided the cipher using correct syntax.
   - Confirm that your browser supports the cipher you provided.
   - Confirm that you do not have other applications installed that redirect or layer additional encryption for SSL traffic.
Perform an Offline Tenable.sc Director Plugin/Feed Updates

You can perform offline plugin or feed updates in air-gapped Tenable.sc Director environments.

- Perform an Offline Nessus Plugin Update
- Perform an Offline NNM Plugin Update
- Perform an Offline Tenable.sc Feed Update

For general information about best practices in air-gapped environments, see Considerations for Air-Gapped Environments.
Perform an Offline Nessus Plugin Update

Required User Role: Administrator

To perform an offline Nessus plugin update:

1. To prevent the Nessus scanner from starting automatically upon restarting the system, run the following command:

```
EL6 > /sbin/chkconfig nessusd off
EL7 > /usr/bin/systemctl disable nessusd
```

2. Run the following command and save the challenge string that is displayed:

```
# /opt/nessus/sbin/nessuscli fetch --challenge
```


   *Note:* Do not click here, even if you have a newer version of Nessus installed. You cannot use the https://plugins.nessus.org/v2/offline.php page for Tenable.sc downloads.

4. Paste the challenge string from Step 3 and your Activation Code in the appropriate boxes on the web page.

5. Click Submit.

6. On the next page, copy the link that starts with https://plugins.nessus.org/get.php... and save it as a favorite. Within the saved link change all-2.0.tar.gz to sc-plugins-diff.tar.gz. This link will be needed for future use.

   *Caution:* Do not click the link for nessus-fetch.rc.

7. Go to the favorite you created.

   The page prompts you to download a file.

8. Download the file, which is called sc-plugins-diff.tar.gz.
9. Verify the file using the MD5 checksum, as described in the [knowledge base](#) article.

10. Save the `sc-plugins-diff.tar.gz` on the system used to access your Tenable.sc Director web interface.

11. Log in to Tenable.sc Director via the user interface.

12. Click **System > Configuration**.

   The **Configuration** page appears.

13. Click **Plugins/Feed**.

   The **Plugins/Feed Configuration** page appears.

14. In the **Schedules** section, expand the **Active Plugins** options.

15. Click **Choose File** and browse to the saved `sc-plugins-diff.tar.gz` file.

16. Click **Submit**.

   After several minutes, the plugin update finishes and the page updates the **Last Updated** date and time.
Perform an Offline NNM Plugin Update

**Required User Role:** Administrator

To perform an offline NNM plugin update:

1. To prevent the NNM scanner from starting automatically upon restarting the system, run the following command:

   ```
   EL6 > /sbin/chkconfig nmm off
   EL7 > /usr/bin/systemctl disable nmm
   ```

2. Run the following command and save the challenge string that is displayed:

   ```
   # /opt/nmm/bin/nmm --challenge
   ```

3. In your browser, navigate to the [NNM plugins page](#).

4. Paste the challenge string from Step 3 and your Activation Code in the appropriate boxes on the web page.

5. Click **Submit**.

6. On the next page, copy the link that starts with [https://plugins.nessus.org/v2/...](#) and bookmark it in your browser. The other information on the page is not relevant for use with Tenable.sc Director.

7. Click the bookmarked link.

   The page prompts you to download a file.

8. Download the file, which is called `sc-passive.tar.gz`.

9. Verify the file using the MD5 checksum, as described in the [knowledge base](#) article.

10. Save the `sc-passive.tar.gz` on the system used to access your Tenable.sc GUI.
11. Log in to Tenable.sc Director via the user interface.

12. Click **System > Configuration**.

   The **Configuration** page appears.

13. Click **Plugins/Feed**.

   The **Plugins/Feed Configuration** page appears.

14. In the **Schedules** section, expand the **Passive Plugins** options.

15. Click **Choose File** and browse to the saved `sc-passive.tar.gz` file.

16. Click **Submit**.

   After several minutes, the plugin update finishes and the page updates the **Last Updated** date and time.
Perform an Offline Tenable.sc Feed Update

**Required User Role:** Administrator

**Note:** If you already performed a Nessus offline plugin update, start at step 7.

To perform an offline Tenable.sc feed update:

1. To prevent the Nessus scanner from starting automatically upon restarting the system, run the following command:

   ```
   EL6 > /sbin/chkconfig nessusd off
   EL7 > /usr/bin/systemctl disable nessusd
   ```

2. Run the following command and save the challenge string that is displayed:

   ```
   # /opt/nessus/sbin/nessuscli fetch --challenge
   ```


4. Paste the challenge string from Step 3 and your Activation Code in the appropriate boxes on the web page.

5. Click **Submit**.


7. Within the saved link change `all-2.0.tar.gz` to `SecurityCenterFeed48.tar.gz`. This link is needed for future use.

   **Caution:** Do not click the link for `nessus-fetch.rc` as it is not needed.

8. Go to the favorite you created.

   The page prompts you to download a file.

9. Download the file, which will be called `SecurityCenterFeed48.tar.gz`.
10. Verify the file using the MD5 checksum, as described in the knowledge base article.

11. Save the SecurityCenterFeed48.tar.gz on the system used to access your Tenable.sc Director GUI.

12. Log in to Tenable.sc Director via the user interface.

13. Click **System > Configuration**.

   The **Configuration** page appears.

14. Click **Plugins/Feed**.

   The **Plugins/Feed Configuration** page appears.

15. In the **Schedules** section, expand the **Tenable.sc Feed** options.

16. Click **Choose File** and browse to the saved SecurityCenterFeed48.tar.gz file.

17. Click **Submit**.

   After several minutes, the plugin update finishes and the page updates the **Last Updated** date and time.
Troubleshooting

This troubleshooting section covers some of the common issues encountered with Tenable.sc Director.

- General Tenable.sc Director Troubleshooting
- Troubleshooting Issues with the custom_CA.inc File
General Tenable.sc Director Troubleshooting

Tenable.sc Director does not appear to be operational

1. If a login page does not appear, close and reopen the web browser.

2. Ensure that the remote httpd service is running on the Tenable.sc Director host:

```
# ps ax | grep httpd
1990 ?   Ss   0:01 /opt/sc/support/bin/httpd -k start
```

3. Ensure that sufficient drive space exists on the Tenable.sc Director host:

```
# df

Filesystem    1K-blocks   Used  Available  Use% Mounted on
/dev/mapper/VolGroup00-LogVol00     8506784     0 8506784     0 /
/dev/sda1         101086  24455  71412  26% /
/Boot            1037732     0     0 /dev/shm
```

4. If there is not enough drive space, recover sufficient space and restart the Tenable.sc Director service:

```
# df

Filesystem    1K-blocks   Used  Available  Use% Mounted on
/dev/mapper/VolGroup00-LogVol00     8506784  6816420  1251276 /
/dev/sda1         101086  24455  71412  26% /boot
/Boot            1037732     0     0 /dev/shm
```
# service SecurityCenter restart

```bash
Shutting down SecurityCenter services: [ OK ]
Starting SecurityCenter services: [ OK ]
```

Locked out of all Tenable.sc Director user accounts

Contact Tenable Support.

Invalid license error

If you receive an invalid license error while attempting to log in as a security manager or lower organizational user, an administrator user must log in and upload a new valid license key. A user with access to the host OS and valid permissions can also check that an up-to-date license exists in `/opt/sc/daemons`. Obtain a license from Tenable and copy it to the daemons directory as the tns user.

```
-rw-r--r--  1 tns tns  1942 Oct 29 12:14 license.key
```

Reporting does not work

Check your Java version. The system only supports OpenJDK and Oracle JRE. The existence of another type of Java on the system will likely break reporting.