Tenable Security Center Director 6.10.x User Guide

Last Revised: November 19, 2026

Copyright © 2026 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Table of Contents

Welcome to Tenable Security Center Director **28**

Tenable Security Center and Tenable Security Center Director 28

Tenable Security Center and Tenable Security Center Director Feature Comparison 28

Get Started With Tenable Security Center Director 29

Prepare 30

Configure Managed Tenable Security Center Instances 30

Install 31

Monitor Scans 32

Refine 33

Expand 33

Considerations for Air-Gapped Environments 34

Tenable Security Center Director Deployments 35

Connect a Managed Tenable Security Center Instance 38

Manage Your Tenable Security Center Instances 40

View Managed Tenable Security Center Instances 41

View Managed Tenable Security Center Instance Details 44

Disconnect a Managed Tenable Security Center Instance 49

Managed Tenable Security Center Instance Settings 50

Requirements 51

Hardware Requirements 52
Storage Requirements 52
CPU and Memory Requirements 53
Disk Space Requirements 54
Network Interface Requirements 63
Cloud Requirements 63
Supported Amazon Machine Images (AMIs) 63
Supported Azure Machine Images 64
Requirements for Tenable Security Center Services in Tenable Enclave Security 65
External PostgreSQL Requirements 65
System Requirements 66
Operating System Requirements 67
SELinux Requirements 67
Secure Environment Requirements 67
Dependencies 68
Tenable Security Center Communications and Directories 70
Tenable Security Center Director Version Requirements 70
Customize SELinux Enforcing Mode Policies for Tenable Security Center Director 71
Use /dev/random for Random Number Data Generation 72
Tenable Security Center Director Database Journaling Modes 72
Enable Write-Ahead Logging 74

Disable Write-Ahead Logging 76
License Requirements 77
Tenable Security Center Versions 78
Licensing Tenable Security Center 78
How Assets are Counted 78
Tenable Security Center Components 80
Reclaiming Licenses 82
Exceeding the License Limit 83
Expired Licenses 83
License Statuses 83
Working with License Keys 84
Apply a New License 85
Update an Existing License 86
Port Requirements 88
Tenable Security Center Instance 88
Tenable Security Center Director 90
Tenable Nessus Scanner 92
Tenable Agent 93
Tenable Network Monitor 94
Browser Requirements 94
Tenable Integrated Product Compatibility 95

Large Enterprise Deployments 96
External PostgreSQL with Tenable Security Center Director 96
Requirements 97
Migration Between Internal and External PostgreSQL 97
Responsibility Matrix 97
Installation 98
Configuration 98
Security 103
Patching and Upgrades 106
Connect an External PostgreSQL Server 106
Backup and Restore Tenable Security Center Director with an External PostgreSQL 108
Installation and Upgrade 109
Before You Install 109
Check System Requirements 109
Understand Tenable Security Center and Tenable Security Center Director Licenses 109
Plan Your Tenable Security Center Director Deployment Version 110
Disable Default Web Servers 110
Modify Security Settings 111
Perform Log File Rotation 111
Allow Tenable Sites 111
Connect a PostgreSQL Server 111

Using the Managed PostgreSQL Server 112
Install Tenable Security Center Director 113
Quick Setup 115
License 115
Connect Tenable Security Center Instances 116
Organization 117
User 117
Review 117
Before You Upgrade 118
Check System Requirements 118
Tenable Security Center Director Upgrade Path 118
Verify Your Plugin Set is Up to Date 118
Plan Your Tenable Security Center Director Deployment Upgrade 119
Java Version Requirements 119
Halt or Complete Running Jobs 119
Perform a Tenable Security Center Director Backup 120
Rename Your Mount Point 121
Verify Your PostgreSQL Server 121
Upgrade Tenable Security Center Director 121
Restore Custom SSL Certificates 124
Update the Apache Configuration File 125

Uninstall Tenable Security Center Director 128
User Access 129
Log In to the Web Interface 130
Log in to the Web Interface via SSL Client Certificate 131
User Roles 134
Manage User Roles 140
Create a User Role 140
View User Role Details 141
Edit a User Role 143
Delete a User Role 144
Organizations and Groups 145
Organizations 145
Organization Settings 146
Groups 151
Group Settings 152
Manage Organizations 153
Add an Organization 153
Edit an Organization 154
View Organization Details 155
Delete an Organization 157
Manage Groups 158

Add a Group 158
View Group Details 158
Delete a Group 159
User Accounts 160
Add a User Account 161
Add a TNS-Authenticated User 161
Add an LDAP-Authenticated User 163
Add a SAML-Authenticated User 165
Manage User Accounts 167
View User Account Details 167
Filter the Users Page 169
Edit Your User Account (Administrator) 170
Edit Your User Account (Organizational User) 171
Replace First User 171
Delete a User Account 173
Linked User Accounts 175
Linked User 175
Linked Non-Admin User 176
Manage Linked Users 177
Add a Linked User 177
Switch to a Linked User Account 178

Edit a Linked User Account (Administrator) 179
Edit a Linked User Account (Linked User) 180
Delete a Linked User Account 180
Custom Group Permissions 182
Manage API Keys 184
Generate API Keys 184
Delete API Keys 185
User Account Options 186
TNS User Account Options 186
LDAP User Account Options 191
SAML User Account Options 194
LDAP Authentication 197
Manage LDAP Servers 202
Add an LDAP Server 202
Delete an LDAP Server 203
LDAP User Provisioning 204
Configure LDAP User Provisioning 205
LDAP Servers with Multiple OUs 207
Option 1 (Recommended) 207
Option 2 208
SAML Authentication 210

Considerations for Advanced SAML Features 210
SAML Authentication Options 213
Configure SAML Authentication Automatically via the User Interface 215
Configure SAML Authentication Manually via the User Interface 217
Configure SAML Authentication via the SimpleSAML Module 219
SAML User Provisioning 223
Configure SAML User Provisioning 224
SAML Authentication XML Configuration Examples 226
OneLogin Example 226
Okta Example 227
Microsoft ADFS Example 229
SSL Client Certificate Authentication 231
Configure Tenable Security Center Director to Allow SSL Client Certificate Authentication 232
Configure a CRL in Tenable Security Center Director 234
Configure OCSP Validation in Tenable Security Center Director 237
Search 238
Certificates and Certificate Authorities in Tenable Security Center Director 241
Tenable Security Center Director Server Certificates 242
Upload a Server Certificate for Tenable Security Center 243
Regenerate the Tenable Security Center Director Server Certificate 245

Trust a Custom CA 247
System Settings 248
Configuration Settings 248
Data Expiration Settings 249
Mail Settings 249
Miscellaneous Settings 251
Web Proxy 251
Syslog 251
Scanning 252
Notifications 253
Report Generation 254
PostgreSQL Connection 255
Privacy 255
License Settings 255
Plugins/Feed Settings 256
SAML Settings 258
Security Settings 258
Edit Plugin and Feed Settings and Schedules 263
Configure Plugin Text Translation 265
API Key Authentication 265
Manage API Key Authentication 266

Enable API Key Authentication ... 266
Disable API Key Authentication ... 267
Diagnostics Settings ... 267
System Status ... 267
Diagnostics File ... 268
Debugging Logs ... 269
Generate a Diagnostics File ... 269
Diagnostics File Options ... 271
Manage Debugging Logs ... 274
Enable Debugging Logs ... 275
Download Debugging Logs ... 276
Disable Debugging Logs ... 276
Job Queue Events ... 277
System Logs ... 277
Publishing Sites Settings ... 278
Keys Settings ... 279
Manage Keys ... 280
Add a Key ... 280
Download the Tenable Security Center Director SSH Key ... 281
Delete a Key ... 281
User Profile Menu Settings ... 282

About ... 282
System Logs (Organizational Users Only) ... 282
Profile (Organizational Users Only) ... 282
Feeds (Organizational Users Only) ... 282
Notifications ... 283
Plugins ... 283
Help ... 284
Logout ... 284
Custom Plugin Packages for NASL and CA Certificate Upload ... 284
custom_feed_info.inc Guidelines ... 285
custom_nasl_archive.tar.gz or custom_nasl_archive.tgz Guidelines ... 285
custom_CA.inc Guidelines ... 285
Manage Custom Plugin Packages ... 288
Create the Custom Plugin Package ... 288
Upload the Custom Plugin Package ... 289
Backup and Restore ... 289
Configuration Backups ... 290
Automatic Backups ... 291
Perform a Backup ... 292
Restore a Backup ... 294
Perform a Configuration Backup ... 295

Restore a Configuration Backup 297

Monitor Scans **301**

Scanning Overview 301

Resources 303

Tenable Nessus Scanners 303

Add a Tenable Nessus Scanner 307

Tenable Nessus Scanner Statuses 310

Manage Nessus Scanners 316

View Your Tenable Nessus Scanners 316

View Details for a Tenable Nessus Scanner 317

Edit a Tenable Nessus Scanner 320

Delete a Tenable Nessus Scanner 320

Pause, Resume, or Stop Scans on a Managed Tenable Security Center Instance 321

Repositories 323

Manage Repositories 324

Add a Repository 324

View Your Repositories 324

View Repository Details 325

Edit a Repository 327

Export a Repository 328

Export via the User Interface 328

Export via the CLI 328
Delete a Repository 330
External Repositories 330
About Remote Repositories 331
Configure a Remote Repository 331
Remote Repositories 332
Active Scan Objects 334
Asset Tags 336
Template-Based Asset Tags 337
Custom Asset Tags 337
Static Asset Tags 337
DNS Name List Asset Tags 338
Combination Asset Tags 338
Dynamic Asset Tags 339
Watchlist Asset Tags 345
Import Asset Tags 346
Manage Asset Tags 346
Add a Template-Based Asset Tag 346
Add a Custom Asset Tag 350
View Asset Tag Details 353
Manage Hosts 354

View Hosts 354
Export Hosts 356
Host Asset Filter Components 356
Audit Files 357
Manage Audit Files 359
Add a Template-Based Audit File 360
Add a Custom Audit File 361
View Audit File Details 362
Edit or Replace Audit Files 363
Share or Revoke Access to Audit Files 364
Export Audit Files 364
Delete Audit Files 365
Scan Zones 366
Manage Scan Zones 369
Add a Scan Zone 369
View Your Scan Zones 370
Edit a Scan Zone 371
Delete a Scan Zone 372
Labels 373
Add a Label 373
Remove or Delete a Label 377

Analyze Data **383**
Trending 383
How Trending Works 383
Why It's Important 384
Requirements and Considerations 384
Dashboards 385
View a Dashboard 387
Insights Dashboard 388
Set a Dashboard as Your Default Dashboard 391
Add a Template-Based Dashboard 392
Add a Custom Dashboard 393
Dashboard and Component Templates 394
Import a Dashboard 396
Manage Dashboards 396
Share or Revoke Access to a Dashboard 398
Delete a Dashboard 399
Manage Dashboard Components 400
Add a Template-Based Dashboard Component 402
Add a Custom Dashboard Component 403
Custom Dashboard Component Options 405
Configure a Simple Matrix Dashboard Component 425

Explore 429
Explore Assets 430
Use the Explore - Assets Page 431
View Asset Details 431
Asset Types 434
Export Assets 445
Explore Assets Export Fields and Associated CSV Keys 446
Asset Filters 456
Asset Columns 459
Explore Findings 460
Use the Findings Page 461
View Findings Details 462
Details 463
Asset Summary 467
Using Group By Options on the Findings Page 468
What is Group By? 468
Using Group By Options 469
Group By Options 469
Group By to Promote Ease of Use 470
Export Findings 471
Findings Filters 472

Findings Columns 477
None 477
Asset 479
Asset Tag 480
CVE 481
IAVM 481
Operating System 482
Severity 483
Vulnerability (Plugin) 483
Scan Results 483
Scan Result Statuses 484
Scan Status 484
Import Status 486
Availability 488
Manage Scan Results 488
View Scan Results 489
View Scan Result Details 490
Filter Scan Results 492
Retrieve a Scan Result From Managed Tenable Security Center 493
Download Scan Results 493
Send a Copy of Scan Results 494

Generate a Report for Scan Results 494
Pause or Resume a Scan 495
Solutions Analysis 495
View Solutions 496
View Solution Details 497
Export Hosts Affected by a Solution 499
Vulnerability Analysis 502
Cumulative vs. Mitigated Vulnerabilities 503
CVSS vs. VPR 504
CVSS 504
Vulnerability Priority Rating 505
VPR Key Drivers 506
Manage Vulnerabilities 508
View Cumulative or Mitigated Vulnerabilities 508
View Vulnerabilities by Host 508
View Vulnerabilities by Plugin 510
View Vulnerability Instance Details 514
Export Vulnerability Data 517
View Host Details 518
View Plugin Details 522
Vulnerability Analysis Tools 523

Vulnerability Analysis Filter Components 529
Vulnerability Intelligence 547
Search Known Vulnerabilities 547
View Vulnerability Profiles 548
Vulnerability Information 548
Events 549
Scores 551
Plugins 552
Products 552
Summary 553
How Does This Affect Me? 553
Sources 553
Vulnerability Metrics 554
General Information 554
Risk Profile 555
Severity Metrics 555
Latest Plugin Coverage 556
Identify Your Exposure 557
Use the Query Builder 558
How Queries Work 558
Build a Query 559

Edit a Query 559
Keyboard Shortcuts 560
Query Builder Filters 560
CVEs 566
My Findings 568
My Affected Assets 570
Plugins 571
Vulnerability Categories 571
Reports 573
Manage Reports 574
Create a Custom Report 574
Create a Template Report 575
Launch a Report on Demand 577
Stop a Running Report 577
Report Templates 578
Data Required for Template-Based Reports 579
Report Options 580
General Options 581
Report Options 582
Definition Options 585
Display Options 587

Distribution Options 588
Manage Report Definitions 589
View a Report Definition 589
Copy a Report Definition 590
Edit a Report Definition 591
Import a Report Definition 591
Export a Report Definition 592
Delete a Report Definition 593
Manage Report Outlines 594
Edit a Report Outline 594
Add a Custom Chapter to a Report 595
Add a Template Chapter to a Report 596
Add or Edit a Report Element 598
Configure a Grouping Element in a Report 599
Configure a Text Element in a Report 604
Configure a Matrix Element in a Report 606
Configure a Table Element in a Report 609
Configure a Charts Element in a Report 612
Reorder Report Chapters and Elements 616
Manage Report Filters 617
Manage Filter Components for a Single Element in a Chapter Report 618

Manage Filter Components for Multiple Elements in a Chapter Report 619
Manage Filter Components for a Non-Chapter Report 621
Manage Report Results 623
View a Report Result 623
Download a Report Result 623
Publish a Report Result 624
Email a Report Result 624
Copy a Report Result 625
View Errors for a Failed Report 626
Delete a Report Result 626
CyberScope and DISA Report Attributes 627
CyberScope Options 627
DISA Options 628
Report Images 629
Filters 630
Apply a Filter 631
Filter Components 632
Queries 636
Manage Queries 637
Add or Save a Query 637
Load a Query 639

Edit a Query 639
Query Options 640
Ticket-Specific Query Options 641
User-Specific Query Options 642
Alert-Specific Query Options 643
Workflow Actions 644
Alerts 644
Alert Actions 644
Alert Options 649
Manage Alerts 651
Add an Alert 651
View Alert Details 652
Edit an Alert 654
Evaluate an Alert 654
Delete an Alert 655
Tickets 656
Manage Tickets 656
Open a Ticket 656
View Ticket Details 657
Edit a Ticket 659
Resolve and Close a Ticket 660

Ticket Options ... 661

Additional Resources ... 663

Start, Stop, or Restart Tenable Security Center Director ... 663

License Declarations ... 664

Encryption Strength ... 665

Configure SSL/TLS Strong Encryption ... 667

File and Process Allow List ... 668

Asset Tracking in Tenable Security Center Director ... 669

Imported Assets ... 670

IPv4 and IPv6 Assets ... 671

Agent Assets ... 672

Offline Plugin and Feed Updates for Tenable Security Center Director ... 673

Perform an Offline Nessus Plugin Update ... 673

Perform an Offline Tenable Network Monitor Plugin Update ... 675

Perform an Offline Tenable Security Center Feed Update ... 677

Migrate Data Between PostgreSQL Implementations ... 679

Migrate from internal PostgreSQL or PostgreSQL 13 through 16 ... 680

Migrate from PostgreSQL 17 ... 682

Troubleshooting ... 684

General Tenable Security Center Director Troubleshooting ... 684

Tenable Security Center Director does not appear to be operational ... 684

Locked out of all Tenable Security Center Director user accounts 685

Invalid license error 685

Reporting does not work 686

Welcome to Tenable Security Center Director

This user guide describes how to install, configure, and manage Tenable Security Center Director™ 6.10.x.

Tenable Security Center Director is an add-on to Tenable Security Center that provides centralized console insight to reduce complexity and give multiple-console customers complete visibility across their entire network.

To get started, see Get Started With Tenable Security Center Director.

For additional information on Tenable Security Center Director, review the following customer education materials:

- Tenable Security Center Director Introduction (Tenable University)

Tenable Security Center and Tenable Security Center Director

Tenable Security Center is a comprehensive vulnerability management solution that provides complete visibility into the security posture of your distributed and complex IT infrastructure. Tenable Security Center consolidates and evaluates vulnerability data from across your entire IT infrastructure, illustrates vulnerability trends over time, and assesses risk with actionable context for effective remediation prioritization.

Tenable Security Center Director is an add-on to Tenable Security Center that provides centralized console insight to reduce complexity and give multiple-console customers complete visibility across their entire network.

Tenable Security Center and Tenable Security Center Director Feature Comparison

Feature	Tenable Security Center	Tenable Security Center Director
Remote repository import (for cumulative data analysis)	X	X
Retrieve data from individual scans		X
Monitor status and configuration of scanning tier instances and connected sensors		X
Centralized scan capability with scanning tiers via the API		X

Get Started With Tenable Security Center Director

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

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

Tip: For additional information on Tenable Security Center Director, review the following customer education materials:

- Tenable Security Center Director Introduction (Tenable University)

Prepare

Before you begin, learn about Tenable Security Center and Tenable Security Center 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. Tenable Security Center Director cannot perform scans. Plan your deployment to ensure you have adequate scan coverage on the Tenable Security Center instances you plan to manage from Tenable Security Center 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 Security Center, see the Tenable Security Center Large Enterprise Deployment Guide.

Configure Managed Tenable Security Center Instances

Configure the Tenable Security Center instances you want to manage with Tenable Security Center Director.

1. Install and fully configure Tenable Security Center on your managed Tenable Security Center instances, as described in Get Started With Tenable Security Center in the *Tenable Security Center User Guide*.

   Note: You must run the same version of Tenable Security Center on your entire Tenable Security Center Director deployment, including Tenable Security Center Director and all managed Tenable Security Center instances that you connect to Tenable Security Center Director. Tenable Security Center Director cannot communicate with managed Tenable Security Center instances that are running a different version of Tenable Security Center.

2. To ensure that your Tenable Security Center instances can connect to Tenable Security Center Director, apply the required license upgrade to each managed Tenable Security Center instance, as described in Update an Existing License in the *Tenable Security Center User Guide*.
3. Generate API keys for an administrator on each managed Tenable Security Center instance, as described in Generate API Keys in the *Tenable Security Center User Guide*.

Install

Install Tenable Security Center Director and perform initial configuration.

Note: You cannot upgrade Tenable Security Center to Tenable Security Center Director. If you want to install Tenable Security Center Director on a host where Tenable Security Center is already installed, you must uninstall Tenable Security Center and perform a clean installation of Tenable Security Center Director on that host. For more information, see Uninstall Tenable Security Center.

Note: You must run the same version of Tenable Security Center on your entire Tenable Security Center Director deployment, including Tenable Security Center Director and all managed Tenable Security Center instances that you connect to Tenable Security Center Director. Tenable Security Center Director cannot communicate with managed Tenable Security Center instances that are running a different version of Tenable Security Center.

1. Prepare for the installation, as described in Before You Install.
2. Install Tenable Security Center Director, as described in Install Tenable Security Center Director.
3. Perform quick setup, as described in Quick Setup. You can:
    - Apply activation codes for Tenable Nessus and Tenable Network Monitor to allow Tenable Security Center Director to perform plugin updates
    - Connect Tenable Security Center instances you want to manage with Tenable Security Center 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 Use the Security section to define the Tenable Security Center user interface login parameters and options for account logins. You can also configure banners, headers, and classification headers and footers..
7. Configure and connect additional managed Tenable Security Center instances, if necessary, as described in Connect a Managed Tenable Security Center Instance.

Monitor Scans

On your managed Tenable Security Center instances, configure and run basic scans, as described in Getting Started with Tenable Security Center in the *Tenable Security Center User Guide*.

In Tenable Security Center Director, monitor running scans and scan results to begin evaluating the effectiveness of your deployment plan and analysis workflow.

- 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.
- Search for vulnerabilities by CVE ID, as described in Search.

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.

Tip: You can manage scan policy configurations for active scans on your managed Tenable Security Center instances from Tenable Security Center Director using the Tenable Security Center Director API. For more information, see the *Tenable Security Center API Guide*.

Refine

Configure other features in Tenable Security Center Director, 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, assets, as described in Add a Custom Asset Tag. For more information about asset types, see Asset Tags.
- 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 Security Center instances and consider revising.
- Review your scan results and scan coverage. You may need to modify your scan configurations on your managed Tenable Security Center 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 Security Center API Guide* and the *Tenable Security Center API Best Practices Guide*.

Considerations for Air-Gapped Environments

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

Architecture

You must deploy a Tenable Security Center 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 Security Center to your other instance of Tenable Security Center. This supports both consolidated and federated reporting structures.

Upgrades and Updates

Tenable recommends performing Tenable Security Center 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, Tenable 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 Security Center upgrade or a plugin/feed update offline:

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

1. Download the files in a browser or via the API.
2. Verify the integrity of the files.
    - Tenable Security Center 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 Security Center instance.
4. Upload the files to Tenable Security Center.
    - Tenable Security Center upgrade: via the CLI.
    - Plugin/feed update: in a browser or via the API.

Tenable Agents

If you deployed Tenable Nessus Manager to manage Tenable 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 Tenable Nessus Manager. Tenable Nessus Manager pushes the update to the managed Tenable Agents.

For more information, see the knowledge base article.

Tenable Security Center Director Deployments

You can use Tenable Security Center Director to manage Tenable Nessus scanners and scan zones and monitor scan results on multiple Tenable Security Center instances. If your deployment includes several instances of Tenable Security Center, Tenable recommends using Tenable Security Center Director to remotely monitor your Tenable Security Center instances.

A Tenable Security Center Director deployment includes:

- One *Tenable Security Center Director* where you connect managed Tenable Security Center instances. You use Tenable Security Center Director to centralize and monitor data collected by your managed Tenable Security Center instances.
  Tenable Security Center Director cannot perform scans. Plan your deployment to ensure you have adequate scan coverage on the Tenable Security Center instances you plan to manage from Tenable Security Center Director.
- One or more *managed Tenable Security Center instances*. You connect managed Tenable Security Center instances to collect vulnerability data that can be viewed in Tenable Security Center Director.

  Note: You must run the same version of Tenable Security Center on your entire Tenable Security Center Director deployment, including Tenable Security Center Director and all managed Tenable Security Center instances that you connect to Tenable Security Center Director. Tenable Security Center Director cannot communicate with managed Tenable Security Center instances that are running a different version of Tenable Security Center.

  Note: To enable cumulative vulnerability data analysis, add the repositories of your managed Tenable Security Center Director instances as Remote Repositories.

To plan and fully configure your Tenable Security Center Director deployment, see Get Started With Tenable Security Center Director.

For more information, see:

- Connect a Managed Tenable Security Center Instance
- Manage Your Tenable Security Center Instances
- Managed Tenable Security Center Instance Settings

Monitor Your Tenable Security Center Director Deployment

After you acquire a Tenable Security Center Director license, configure Tenable Security Center Director, and connect one or more managed Tenable Security Center instances, you can monitor the following details from Tenable Security Center Director:

- The status, version, and total number of Tenable Nessus Scanners running on each managed Tenable Security Center instance
- The Scan Zones configured on each managed Tenable Security Center instance
- The scan results of scans run on each managed Tenable Security Center instance
- A summary of plugin sets used on each managed Tenable Security Center instance
- A summary of plugin sets used by Tenable Nessus scanners on each managed Tenable Security Center instance
- The version of Tenable Security Center running on each managed Tenable Security Center instance

You can configure the following from Tenable Security Center Director:

- Add, edit, and delete Tenable Nessus scanners and scan zones on managed Tenable Security Center instances. For more information, see Tenable Nessus Scanners and Scan Zones.
- Pause, resume, or stop scans that are running on managed Tenable Security Center instances, as described in Pause, Resume, or Stop Scans on a Managed Tenable Security Center Instance.

Note: You can only edit configurations for Tenable Nessus scanners and scan zones on managed Tenable Security Center instances from Tenable Security Center Director. To manage other configurations on a managed Tenable Security Center instance, log in to that instance.

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

Tip: Managed Tenable Security Center instances cannot share repository data. For more information about sharing repository data between Tenable Security Center instances, see Tiered Remote Repositories.

Tip: Using the Tenable Security Center Director API, you can perform the following actions to manage active scans on your managed Tenable Security Center instances:

- Add, retrieve, and delete scan and scan policy configurations for active scans.
- Retrieve scan objects, such as users, scan policies, repositories, and scan zones for active scans.

For more information, see the *Tenable Security Center API Guide*.

Connect a Managed Tenable Security Center Instance

Required Tenable Security Center Director User Role: Administrator

For more information about using Tenable Security Center Director to monitor your Tenable Security Center instances, see Tenable Security Center Director Deployments.

Before you begin:

1. If you are connecting an existing Tenable Security Center instance to Tenable Security Center Director for the first time, confirm that the instance has a **Managed Tenable Security Center** license. To obtain the updated license key:
   a. Log in to the Tenable Account Management portal.
   b. Locate the Tenable Security Center instance and click **Download License Key**.
   c. Apply the new license key to the Tenable Security Center instance, as described in Update an Existing License.

   Note: For new Tenable Security Center instances that you are setting up as managed instances, Tenable automatically applies the required license when you purchase a Tenable Security Center Director license. No additional license steps are required.

2. Confirm the Tenable Security Center instance you want to connect to Tenable Security Center Director is running the same Tenable Security Center version as Tenable Security Center

Director. You must run the same version of Tenable Security Center on your entire Tenable Security Center Director deployment, including Tenable Security Center Director and all managed Tenable Security Center instances that you connect to Tenable Security Center Director. Tenable Security Center Director cannot communicate with managed Tenable Security Center instances that are running a different version of Tenable Security Center.

3. Generate API keys for an administrator on the Tenable Security Center instance you want to manage with Tenable Security Center Director, as described in Generate API Keys in the *Tenable Security Center User Guide*.

To connect a Tenable Security Center instance to Tenable Security Center Director:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Managed Instances**.

   The **Tenable Security Center Instances** page appears.
3. Click the **Add** button.

   The **Add Tenable Security Center Instance** page appears.
4. Configure the options for the managed Tenable Security Center instance. For more information, see Managed Tenable Security Center Instance Settings.
   a. In the **Name** box, type a name for the Tenable Security Center instance.
   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 Security Center instance, enable the **Verify Hostname** toggle.
   h. (Optional) To use the proxy configured in Tenable Security Center Director for communication with the Tenable Security Center instance, enable the **Use Proxy** toggle.

5. Click **Submit**.

   Tenable Security Center Director saves your configuration.

What to do next:

- Begin monitoring data on your managed Tenable Security Center instances.
  - To view the Tenable Nessus scanners, scan zones, and scan results on a managed Tenable Security Center instance, see View Managed Tenable Security Center Instance Details.
  - To view the Tenable Nessus scanners on your managed Tenable Security Center instances, see View Your Tenable Nessus Scanners.
  - To view the scan zones on your managed Tenable Security Center instances, see View Your Scan Zones.
  - To view the scan results on your managed Tenable Security Center instances, see View Scan Results.

Manage Your Tenable Security Center Instances

Required Tenable Security Center Director User Role: Administrator

For more information about using Tenable Security Center Director to monitor your Tenable Security Center instances, see Tenable Security Center Director Deployments.

To manage your linked Tenable Security Center instances:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Managed Instances**.

   The **Tenable Security Center Instances** page appears.
3. To view the list and status of your managed Tenable Security Center instances, see View Managed Tenable Security Center Instances.
4. To view details for a managed Tenable Security Center instance, see View Managed Tenable Security Center Instance Details.

5. To edit the settings for a managed Tenable Security Center instance:
    a. Right-click the row for the managed Tenable Security Center instance you want to edit.

       The actions menu appears.
    b. Click **Edit**.

       The **Edit Tenable Security Center Instance** page appears.
    c. Modify the managed Tenable Security Center instance options. For more information, see Managed Tenable Security Center Instance Settings.
    d. Click **Submit**.

       Tenable Security Center Director saves your configuration.
6. To disconnect a managed Tenable Security Center instance, see Disconnect a Managed Tenable Security Center Instance.

View Managed Tenable Security Center Instances

Required Tenable Security Center Director User Role: Administrator

You can view an overview of basic information about your managed Tenable Security Center instances from Tenable Security Center Director. To view more details about an instance, see View Managed Tenable Security Center Instance Details.

For more information about using Tenable Security Center Director to monitor your Tenable Security Center instances, see Tenable Security Center Director Deployments.

To view a list of your managed Tenable Security Center instances:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Managed Instances**.

   The **Tenable Security Center Instances** page appears.
3. View the following information about each managed Tenable Security Center instance:

- **Name** – The name of the instance.
- **IP/FQDN** – The IP address of the instance.
- **Version** – The version of Tenable Security Center running on the instance.
- **Status** – The status of the scanners on the instance.

Status	Description	Recommended Action
Working	All of the scanners configured on the managed Tenable Security Center instance are **Working**.	None.
***x*/*y* Scanners Available**	Only some of the scanners configured on the managed Tenable Security Center instance are **Working**. The status label shows the number of **Working** scanners compared to the total number of scanners on the managed Tenable Security Center instance.	Review your scanner statuses to identify the scanners with issues, as described in View Your Tenable Nessus Scanners. Then, follow the recommended actions to resolve the issues, as described in Tenable Nessus Scanner Statuses.
Connection Error	Tenable Security Center Director cannot communicate with the managed Tenable	None.

	Security Center instance.	
Protocol Error	The provided credentials for the Tenable Security Center instance are invalid.	Edit the managed Tenable Security Center instance in Tenable Security Center Director to add a valid API **Access Key** and **Secret Key** for the managed Tenable Security Center instance. To generate a new API access key and secret key for the Tenable Security Center instance, see Generate API Keys in the *Tenable Security Center User Guide*.

- **Scanners** – The number of available scanners compared to the total number of scanners on the managed Tenable Security Center instance.
- **Last Sync** – The date and time Tenable Security Center Director successfully synchronized with the managed Tenable Security Center instance. Tenable Security Center Director syncs with managed Tenable Security Center instances every 15 minutes.

View Managed Tenable Security Center Instance Details

Required Tenable Security Center Director User Role: Administrator

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

For more information about managing Tenable Security Center instances with Tenable Security Center Director, see Tenable Security Center Director Deployments.

To view details for a managed Tenable Security Center instance:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Managed Instances**.

   The **Tenable Security Center Instances** page appears.
3. Right-click the row for the managed Tenable Security Center instance.

   The actions menu appears.

   -or-

   Select the check box for the managed Tenable Security Center instance.

   The available actions appear at the top of the table.
4. Click **View**.

   The managed Tenable Security Center instance page appears.
5. ### To view configuration details for the managed Tenable Security Center instance:

   a. Click the **Information** tab.

      The **Information** tab appears.

   b. View the following information for the managed Tenable Security Center instance:

Section	Action

General	View general information about the managed Tenable Security Center instance.
Options	View optional settings configured for the managed Tenable Security Center instance. For more information, see Managed Tenable Security Center Instance Settings.
Scanner Summary	View a summary of the scanners configured on the managed Tenable Security Center instance. • **Scanner Version** – The total number of Tenable Nessus scanners on the instance, organized by Tenable Nessus scanner version. • **Scanner Status** – The total number of Tenable Nessus scanners on the instance, organized by scanner status. For more information about a status, see Tenable Nessus Scanner Statuses. • **Scanner PluginSet** – The total number of Tenable Nessus scanners on the instance, organized by scanner plugin set.

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

   a. Click the **Scanners** tab.

      The **Scanners** tab loads.

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

Section	Action
Scanners	• View the number of operational Tenable Nessus scanners

table	compared to the total number of scanners on the managed Tenable Security Center instance.
	• View the Tenable Nessus scanners on the managed Tenable Security Center instance.
	  • **Name** – The name for the scanner.
	  • **Features** – Specifies whether the scanner is a **Standard** scanner or an **Agent Capable** scanner. Agent capable scanners provide Tenable Agent scan results to Tenable Security Center.
	  • **Status** – The status of the scanner.
	  • **Host** – The IP address or hostname of the scanner.
	  • **Version** – The scanner's Tenable Nessus version.
	  • **Type** – The type of scanner connection: **Tenable Nessus (Unmanaged Plugins)** or **Tenable Nessus (Managed Plugins)**. For more information, see View Your Tenable Nessus Scanners.
	  • **Uptime** – The length of time, in days, that the scanner has been running.
	  • **Last Modified** – The date and time the scanner was last modified.
	• View details for a Tenable Nessus scanner on the managed Tenable Security Center instance.
	  1. Right-click the row for the scanner you want to view.
	  The actions menu appears.
	  2. Click **View**.
	  The **View Tenable Nessus Scanner** page appears. For

	more information, see View Details for a Tenable Nessus Scanner.

7. To view the scan zones configured on the managed Tenable Security Center 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:

Section	Action

Scan Zones table	• View the number of operational scan zones on the managed Tenable Security Center instance.
	• View the scan zones on the managed Tenable Security Center instance.
	  • **Name** – The name for the scan zone.
	  • **Status** – The status of the scan zone. For more information, see View Your Scan Zones.
	  • **Scanners** – The number of Tenable 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 Security Center instance.
	  1. Right-click 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 Security Center 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 Security Center instance.
	  • **Name** – The name for the scan associated with the result.
	  • **Availability** – The status of the scan result. For more information, see Scan Result Statuses.
	  • **Type** – The type of scan that generated the scan result.
	  • **Scan Policy** – The name of the scan policy that generated the scan result.
	  • **Scanned IPs** – The number of IP addresses scanned.
	  • **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 Security Center 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 Security Center instances from the past 7 days. To view older scan results, log in to the managed Tenable Security Center instance where the scan took place.
	• View details for a scan result on the managed Tenable Security Center instance.
	  • 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 Security Center instance:
   a. Click the **Jump to** menu.
   The list of managed Tenable Security Center instances appears.
   b. Click the name of the managed Tenable Security Center instance you want to view.
   The **View Tenable Security Center Instance** page appears.

Disconnect a Managed Tenable Security Center Instance

Required Tenable Security Center Director User Role: Administrator

Disconnect a managed Tenable Security Center instance from Tenable Security Center Director to stop monitoring the instance from Tenable Security Center Director. You can continue using individual Tenable Security Center instances separately from Tenable Security Center Director. For more information, see Tenable Security Center Director Deployments.

To disconnect a managed Tenable Security Center instance:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Managed Instances**.
   The **Tenable Security Center Instances** page appears.
3. Right-click the row for the managed Tenable Security Center instance you want to disconnect.

The actions menu appears.

-or-

Select the check box for the managed Tenable Security Center instance you want to disconnect.

The available actions appear at the top of the table.

4. Click **Delete**.

   A confirmation window appears.

5. Click **Delete**.

   Tenable Security Center Director disconnects the managed Tenable Security Center instance.

Managed Tenable Security Center Instance Settings

For more information about using Tenable Security Center Director to monitor your Tenable Security Center instances, see Tenable Security Center Director Deployments.

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

Option	Description
General	
Name	A descriptive name for the Tenable Security Center instance.
IP Address	The IP address of the Tenable Security Center instance.
Port	The TCP port that the Tenable Security Center instance listens on for communications from Tenable Security Center Director (443).
Description	(Optional) A description for the Tenable Security Center instance.
API Keys	

Option	Description
Access Key	The API access key for an administrator user on the managed Tenable Security Center instance. For more information, see Manage API Keys.
Secret Key	The API secret key for an administrator user on the managed Tenable Security Center instance. For more information, see Manage API Keys.
Options	
Verify Hostname	(Optional) When enabled, adds a check to verify that the IP address entered in the **IP Address** option matches the Common Name (CN) presented in the SSL certificate from the managed Tenable Security Center instance.
Use Proxy	(Optional) When enabled, instructs Tenable Security Center Director to use its configured proxy for communication with the managed Tenable Security Center instance.

Requirements

You can run Tenable Security Center Director in the following environments.

Environment			More Information
Tenable Core	Virtual	VMware	Requirements in the *Tenable Core User Guide*
		Microsoft Hyper-V	
	Cloud	Amazon Web Services (AWS)	
	Hardware		

Other platforms	Cloud	Amazon Web Services (AWS)	Cloud Requirements
	Hardware		Hardware Requirements

For general information about other requirements to run Tenable Security Center Director, see:

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

Hardware Requirements

You can run Tenable Security Center on hardware, with or without Tenable Core. For more information about Tenable Core, see the Tenable Core User Guide.

Note: Tenable strongly discourages running Tenable Security Center or Tenable Core + Tenable Security Center in an environment shared with other Tenable applications.

Note: Complex deployments require more resources. For example, deployments with large numbers of organizations or application objects. For more information, see Performance in the *Tenable Security Center Large Deployment Guide*.

Storage Requirements

Tenable recommends installing Tenable Security Center 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 Security Center on network-attached storage (NAS), including network filesystems such as NFS.

CPU and Memory Requirements

The CPU core and memory values in the following tables are minimum recommendations for the number of active IPs that Tenable Security Center manages. The disk space tables in the following section do not include CPU or memory.

> **Note:** Tenable Security Center recommends a minimum of 16 GB RAM for all installations. Tenable Security Center will not operate with less than 8 GB (8192 MiB) RAM. See the following tables for recommended CPU and memory by deployment size.

Requirements When Running Basic Network Scans + Local Checks

# of Hosts Managed by Tenable Security Center	CPU Cores	Memory
1 to 2,500	8 2GHz cores	16 GB RAM
2,501 to 10,000	16 3GHz cores	32 GB RAM
10,001 to 25,000	32 3GHz cores	64 GB RAM
25,001 to 100,000	48 3GHz cores	96 GB RAM

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

# of Hosts Managed by Tenable Security Center	CPU Cores	Memory
1 to 2,500	8 2GHz cores	16 GB RAM
2,501 to 10,000	16 3GHz cores	32 GB RAM
10,001 to 25,000	32 3GHz cores	64 GB RAM
25,001 to 100,000	48 3GHz cores	128 GB RAM

Factors That Increase CPU and Memory Requirements

Complex deployments require more CPU and memory than the values in the tables. Consider the following factors when sizing your deployment:

- The number of organizations
- The number of reports that run concurrently
- The number of scans that run concurrently
- Scan result retention and trending depth
- The number of application objects, such as dashboards, reports, assets, and scan policies

For deployments that exceed 100,000 active IPs, you must use an external PostgreSQL instance. For more information, see External PostgreSQL Requirements.

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 are heavily based on the former. Disk space requirements vary depending on usage based on the amount and length of time data is stored on the system.

Disk requirements for Tenable Security Center 6.9 and later are primarily driven by **scan result storage**.

Estimation only: Many factors influence actual disk usage, including scan plugin selection, the number and types of findings per host, scan concurrency, the number of repositories, organization count, and configured retention periods. The values in this section are high-water-mark estimates intended for capacity planning purposes. Actual usage will vary. Monitor disk utilization after deployment and adjust retention settings as needed.

Tenable recommends installing Tenable Security Center on direct-attached storage (DAS) or a SAN with latency of 10 milliseconds or less. NAS and NFS are not supported. High-performance disks (SSDs) are strongly recommended. The `/opt` partition should reside on a dedicated disk or partition separate from the operating system.

Disk Space Components

Component	Size	Notes
Scan result storage	Scales with host count, scan frequency, and retention	Dominant driver. See sizing tables below.
Repository data	~1.1 MB per host (with local checks) ~2.3 MB per host (with local checks and 1 compliance audit)	Stored both in files on disk and in the local PostgreSQL database.
OS, plugins, and application databases	~25 GB	Base install included in the sizing tables below.
Active scan temp space	150 GB baseline (peak; scales with deployment)	Ephemeral. Required under `/opt` during active scans.
Upgrade temp space	~10 GB	Required in `/tmp` during upgrades.

Scope and Assumptions

The sizing tables in this section depend on the following conditions:

- Nessus scanners are directly attached and scan attachments are disabled. If you use linked scanners or enable plugin attachments, see Linked Scanners or Enabling Plugin Attachments.
- Scans run weekly with a 60-day retention period (9 scans stored).
- Each host has a high-water mark of 250 findings per scan.
- The 150 GB of active scan temp space is a baseline, not a ceiling. Large scans and multiple concurrent scans can use more.

Scan Result Sizing

The following tables show total disk requirements for the scope and assumptions above. A host with 250 findings corresponds to roughly 500 KB of scan result data. The tables use 30 MB per 50 hosts per scan (0.6 MB per host) to leave a small buffer. Each row is sized at the upper bound of its host range. For example, the 1 to 2,500 row is sized for 2,500 hosts.

Basic Network Scans + Local Checks (Credentialed)

# of Hosts Managed by Tenable Security Center	Repository Data	Scan Results (9 scans)	Base Install	Minimum Total Disk Required
1 to 2,500	2.75 GB	13.5 GB	25 GB	**41 GB**
2,501 to 10,000	11 GB	54 GB	25 GB	**90 GB**
10,001 to 25,000	27.5 GB	135 GB	25 GB	**188 GB**
25,001 to 50,000	55 GB	270 GB	25 GB	**350 GB**
50,001 to 100,000	110 GB	540 GB	25 GB	**675 GB**

Basic Network Scans + Local Checks + 1 Configuration Audit

# of Hosts Managed by Tenable Security Center	Repository Data	Scan Results (9 scans)	Base Install	Minimum Total Disk Required
1 to 2,500	5.75 GB	40.5 GB	25 GB	**72 GB**
2,501 to 10,000	23 GB	162 GB	25 GB	**210 GB**
10,001 to 25,000	57.5 GB	405 GB	25 GB	**488 GB**
25,001 to 50,000	115 GB	810 GB	25 GB	**950 GB**
50,001 to 100,000	230 GB	1.62 TB	25 GB	**1.88 TB**

Note: Add at least 150 GB of additional headroom for active scan temp space. The 150 GB figure is a baseline, not a ceiling: large scans and multiple concurrent scans can require more. This space is reclaimed after scans complete but must be available on the `/opt` partition during scanning.

Adjusting for Scan Frequency and Retention

The tables above assume weekly scans with a 60-day retention period. To calculate disk requirements for different configurations, use the following approach:

- **Scan results per year:** (scans per week) × 52 × (assets ÷ 50) × 30 MB
- **Retention adjustment:** Multiply by (scans retained ÷ (scans per week × 52)). Scans retained is the number of scans stored within your retention period, rounded up from your retention days. For example, 60 days of retention at one scan per week is 9 scans retained, and 63 days of retention at two scans per week is 18 scans retained. The result equals scans retained × (assets ÷ 50) × 30 MB.
- **Compliance audit adjustment:** For environments running basic network scans plus one configuration audit, use 90 MB per 50 assets per scan instead of 30 MB (1.8 MB per host per scan). Audit results carry more content per finding and grow as audit files add checks.

Note: The tables in this section use 60-day retention as the sizing example (9 weekly scans stored). At the default retention of 365 days, multiply the scan result storage figures by approximately 6× (52

scans stored instead of 9). Reducing retention from the default is the most effective way to control disk consumption.

Linked Scanners or Enabling Plugin Attachments

When using linked scanners or when plugin attachments are enabled, scan results take up significantly more disk space than the directly attached baseline. Use the following per-host estimates when sizing scan result storage:

- **Credentialed vulnerability scans:** 4 MB per host per scan
- **Configuration audits:** 2 MB per host per scan

For example, a weekly scan of 2,500 hosts with 60-day retention (9 scans) requires approximately 90 GB of scan result storage for credentialed vulnerability scans. Multiply by your host count, scan frequency, and configured retention period to determine total allocation.

For a combined credentialed vulnerability scan and one configuration audit, use 6 MB per host per scan (4 MB + 2 MB); a weekly scan of 2,500 hosts with 60-day retention (9 scans) requires approximately 135 GB of scan result storage. Multiply by your host count, scan frequency, and configured retention period to determine total allocation.

Amazon EC2 Instance Type Sizing Tables

Requirements When Running Basic Network Scans + Local Checks

# of Hosts Managed by Tenable Security Center	EC2 Instance Type	vCPU	RAM
1 to 2,500	m5.2xlarge	8	32 GB
2,501 to 10,000	m5.4xlarge	16	64 GB
10,001 to 25,000	m5.8xlarge	32	128 GB
25,001 to 50,000	m5.12xlarge	48	192 GB

# of Hosts Managed by Tenable Security Center	EC2 Instance Type	vCPU	RAM
50,001 or more	For assistance with large enterprise deployments greater than 50,000 active IP addresses, contact your Tenable representative.		

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

# of Hosts Managed by Tenable Security Center	EC2 Instance Type	vCPU	RAM
1 to 2,500	m5.2xlarge	8	32 GB
2,501 to 10,000	m5.4xlarge	16	64 GB
10,001 to 25,000	m5.8xlarge	32	128 GB
25,001 to 50,000	m5.12xlarge	48	192 GB
50,001 or more	For assistance with large enterprise deployments greater than 50,000 active IP addresses, contact your Tenable representative.		

Supported Azure Instance Types

You can install Tenable Security Center in an Azure Virtual Machine (Azure Virtual Image) cloud-based environment that meets all of the following requirements. Tenable recommends the following virtual machine instance types based on your Tenable Security Center deployment size. You may need to increase the storage allocated to the virtual machine instance depending on usage.

Requirements When Running Basic Network Scans + Local Checks

# of Hosts Managed by Tenable Security Center	Virtual Machine Instance	vCPU	RAM
1 to 2,500	D8s_v6	8	32 GB
2,501 to 10,000	D16s_v6	16	64 GB
10,001 to 25,000	D32s_v6	32	128 GB
25,001 to 50,000	D48s_v6	48	192 GB
50,001 or more	For assistance with large enterprise deployments greater than 50,000 active IP addresses, contact your Tenable representative.		

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

# of Hosts Managed by Tenable Security Center	Virtual Machine Instance	vCPU	RAM
1 to 2,500	D8s_v6	8	32 GB
2,501 to 10,000	D16s_v6	16	64 GB
10,001 to 25,000	D32s_v6	32	128 GB
25,001 to 50,000	D48s_v6	48	192 GB
50,001 or more	For assistance with large enterprise deployments greater than 50,000 active IP addresses, contact your Tenable representative.		

Supported Google Cloud Platform (GCP) Instance Types

You can install Tenable Security Center in a GCP cloud-based environment that meets all of the following requirements. Tenable Security Center uses a balance of networking and compute

resources and requires persistent storage for proper operation. Tenable recommends the following GCP instance types based on your Tenable Security Center deployment size.

Requirements When Running Basic Network Scans + Local Checks

# of Hosts Managed by Tenable Security Center	GCP Instance Type	vCPU	RAM
1 to 2,500	c4a-standard-8	8	32 GB
2,501 to 10,000	c4a-standard-16	16	64 GB
10,001 to 25,000	c4a-standard-32	32	128 GB
25,001 to 50,000	c4a-standard-48	48	192 GB
50,001 or more	For assistance with large enterprise deployments greater than 50,000 active IP addresses, contact your Tenable representative.		

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

# of Hosts Managed by Tenable Security Center	GCP Instance Type	vCPU	RAM
1 to 2,500	c4a-standard-8	8	32 GB
2,501 to 10,000	c4a-standard-16	16	64 GB
10,001 to 25,000	c4a-standard-32	32	128 GB
25,001 to 50,000	c4a-standard-48	48	192 GB
50,001 or more	For assistance with large enterprise deployments greater than 50,000 active IP addresses, contact your Tenable representative.		

External PostgreSQL

Deployments exceeding 100,000 active IPs require an external PostgreSQL instance. Repository data, trending results, and configuration data are stored in PostgreSQL. Size the external PostgreSQL instance using the External PostgreSQL Requirements table, and account for growth as scan and configuration data accumulates over time. The disk totals in this section cover the Tenable Security Center host only and do not include the external PostgreSQL instance.

Disk Partition Requirements

Note: When you upgrade to or install Tenable Security Center version 6.10.x and run the RPM from the `/tmp` folder, you must have at least 10 GB of space in the `/tmp` folder if the `/tmp` folder is in its own partition. If the `/tmp` folder does not have enough space, the installation or upgrade fails.

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

Deploying Tenable Security Center 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 Security Center 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 Security Center server. This is to increase the overall performance of web sessions, emails, and other network activities.

Cloud Requirements

The primary method to deploy Tenable Security Center in a cloud environment is with Tenable Core + Tenable Security Center. For more information, see the Tenable Core User Guide.

However, you can install Tenable Security Center in vendor-supported version of your cloud environment that meets the operating system requirements to run Tenable Security Center.

The following guidelines can help you install Tenable Security Center in an Amazon Elastic Compute Cloud (Amazon EC2) cloud-based environment or an Azure Virtual Machine (Azure Virtual Image) 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.

For recommended cloud instance types and sizing, see Hardware Requirements.

Supported Amazon Machine Images (AMIs)

Tenable provides an AMI for Tenable Core, but not for other cloud deployments without Tenable Core. Tenable supports using the following Amazon Marketplace AMI for Tenable Security Center without Tenable Core:

- CentOS Stream 9 (x86_64)
- Red Hat Enterprise Linux 9
- Red Hat Enterprise Linux 8

Configuration considerations:

- These AMIs may not include Java, but Tenable Security Center requires OpenJDK or the Oracle Java JRE to export PDF reports.

  You must install OpenJDK or the Oracle Java JRE onto your AMI before hosting Tenable Security Center. For more information, see Dependencies.
- These AMIs may configure an SELinux enforcing mode policy, which requires customization to be compatible with Tenable Security Center.

  You must use the SELinux `sealert` tool to identify errors and solutions. For more information, see Customize SELinux Enforcing Mode Policies for Tenable Security Center.
- You must confirm these AMIs meet all other standard requirements for operating systems. For more information, see Operating System Requirements.

Supported Azure Machine Images

Tenable provides an Azure image for Tenable Core, but not for other cloud deployments without Tenable Core. Tenable supports using the following Azure images for Tenable Security Center:

- Oracle Linux 8 or 9 VM
- Red Hat Enterprise Linux 8 or 9 VM

Configuration considerations:

- These images may not include Java, but Tenable Security Center requires OpenJDK or the Oracle Java JRE to export PDF reports.

  You must install OpenJDK or the Oracle Java JRE onto your image before hosting Tenable Security Center. For more information, see Dependencies.

- These images may configure an SELinux enforcing mode policy, which requires customization to be compatible with Tenable Security Center.

  You must use the SELinux `sealert` tool to identify errors and solutions. For more information, see Customize SELinux Enforcing Mode Policies for Tenable Security Center.

- You must confirm these images meet all other standard requirements for operating systems. For more information, see Operating System Requirements.

Requirements for Tenable Security Center Services in Tenable Enclave Security

Service	# of Hosts Managed by Tenable Security Center	CPU per pod	Memory per pod	Default pod replicas	Disk space
Reporting pod	1 to 2,500 active IPs	4 cores	8 GiB	1 per report (max 4)	Uses cluster storage dedicated for the pod until report completion
	2,501 to 10,000 active IPs	8 cores	16 GiB		
	10,001 to 25,000 active IPs	16 cores	32 GiB		
	25,001 to 50,000 active IPs	24 cores	48GiB		
Job manager pod	1 to 50,000 active IPs	4 cores	4 GiB	1	N/A

External PostgreSQL Requirements

You can install Tenable Security Center configured to work with a PostgreSQL instance managed by you. PostgreSQL is required for certain features. For more information about connecting a PostgreSQL database, see Connect an External PostgreSQL Server.

This is a required configuration if you have more than 100K hosts. Tenable Security Center requires PostgreSQLversions 13 through 17. It is also recommended that `wal_segment_size` is set to be at least 64MB.

If you set up your PostgreSQL instance in a cloud environment, the following are guidelines for choosing your instance size. Note that the disk space in the following table is only for PostgreSQL data, and does not include any other OS or other dependencies you have.

# of Hosts Managed by Tenable Security Center	AWS	Azure	Google Cloud Platform (GCP)	Minimum Disk Space Required for PostgreSQL Data
1 to 2,500 active IPs	m6g.xlarge	D4s_v3	t2a-standard-4	20 GB
2,501 to 10,000 active IPs	m6g.2xlarge	D16s_v3	t2a-standard-8	50 GB
10,001 to 25,000 active IPs	m6g.4xlarge	D32s_v3	t2a-standard-16	100 GB
25,001 to 100,000 active IPs	m6g.8xlarge	D48s_v3	t2a-standard-32	400GB
100,001 to 250,000 active IPs	m6g.16xlarge	D64s_v3	t2a-standard-48	1 TB

System Requirements

Operating System Requirements

This version of Tenable Security Center is available for:

- Red Hat Enterprise Linux 8 (RHEL 8), 64-bit
- Red Hat Enterprise Linux 9 (RHEL 9), 64-bit
- CentOS Stream 9, 64-bit
- Oracle Linux 8, 64-bit
- Oracle Linux 9, 64-bit

SELinux Requirements

Tenable Security Center 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 Security Center.
- Enforcing mode policies require customization to interact with Tenable Security Center. For more information, see Customize SELinux Enforcing Mode Policies for Tenable Security Center 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 Security Center 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 Security Center may not log audit data during system administrator troubleshooting or other activities. For more information about troubleshooting resource exhaustion, see General Tenable Security Center Director Troubleshooting.

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

> **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 Security Center have an established and applied IT management policy that covers system administration integrity, resource monitoring, physical security, and disaster recovery.

Dependencies

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

- 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.
- You must upgrade pyTenable to version 1.4.2 or later.
- To run Tenable Security Center, you must install `binutils` and `initscripts`. If you try to migrate from Tenable Security Center 5.23.x or earlier to a current version of Tenable Security Center on a system that does not have `binutils` or `initscripts` installed, the migration will

fail.

- You must install `tar`. This is required for extracting and managing compressed archive files during installation and updates.

Note: Tenable recommends using the latest stable production version of each package.

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 readily apparent with a wide variety of functions. Tenable Support has observed different types of failure modes for Tenable Security Center when dependencies are missing.

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

```
# yum deplist SecurityCenter-x.x.x-el6.x86_64.rpm
```

- or -

```
# dnf deplist SecurityCenter-x.x.x-el8.x86_64.rpm
```

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):

```
# yum list installed | grep libtool
```

- or -

```
# dnf list installed | grep libtool
```

If one of the prerequisite packages is missing, it can be installed using the “yum” or “dnf” package managers. For example, install Java 1.8.0 with “yum” using the command below:

```
# yum -y install java-1.8.0-openjdk.x86_64
```

Tenable Security Center Communications and Directories

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

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

Tenable Security Center Directories	
Installation Directory	`/opt/sc`
User Data	`/opt/sc/orgs/<Organization Serial Number>`
Repositories	`/opt/sc/repositories/<Repository Number>`
Admin Logs	`/opt/sc/admin/logs/`
Organization Logs	`/opt/sc/orgs/<Organization Number>/logs/`
Communication Interfaces	• User Access – HTTPS • Feed Updates – Acquired over SSL from Tenable servers directly to Tenable Security Center 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 Security Center, see Encryption Strength.

Tenable Security Center Director Version Requirements

You must run the same version of Tenable Security Center on your entire Tenable Security Center Director deployment, including Tenable Security Center Director and all managed Tenable Security

Center instances that you connect to Tenable Security Center Director. Tenable Security Center Director cannot communicate with managed Tenable Security Center instances that are running a different version of Tenable Security Center.

Customize SELinux Enforcing Mode Policies for Tenable Security Center Director

Security-Enhanced Linux (SELinux) enforcing mode policies require customization to interact with Tenable Security Center 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:

   ```
   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 Security Center Director, as described in Start, Stop, or Restart Tenable Security Center Director.

   Tenable Security Center Director restarts.
4. Run the `sealert` tool again to confirm you resolved the error alerts.

Use /dev/random for Random Number Data Generation

Required Tenable Security Center User Role: Root user

If your organization requires Tenable Security Center 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 Security Center Director:

1. Log in to Tenable Security Center Director via the command line interface (CLI).
2. In the CLI in Tenable Security Center Director, run the following command:

   ```
   export TSC_ENTROPY_CHECK=true
   ```

   Tenable Security Center Director recognizes the environment variable and uses `/dev/random`.

What to do next:

- Install or upgrade Tenable Security Center Director in order for your changes to take effect, as described in Install Tenable Security Center Director or Upgrade Tenable Security Center Director.

Tenable Security Center Director Database Journaling Modes

By default, Tenable Security Center Director databases that can significantly impact performance use write-ahead logging (WAL) journaling mode. All other databases use DELETE mode. Tenable Security Center Director also supports converting WAL journaling mode databases to DELETE mode.

For Tenable Security Center installations where WAL is not enabled, enabling WAL may resolve issues with excessive database locks. If your Tenable Security Center Director does not experience database locking issues, Tenable recommends leaving your Tenable Security Center Director databases in the default journaling mode.

Tenable strongly recommends performing a backup before converting database journaling modes and performing regular backups after converting database journaling modes. For more information, see Backup and Restore.

For general information about SQLite3 database journaling modes, see the SQLite3 documentation.

For more information, see:

- Enable Write-Ahead Logging
- Disable Write-Ahead Logging

Note: If you previously converted one or more Tenable Security Center Director databases to WAL journaling mode without using the `convertDatabaseMode.php` script, you must use the `convertDatabaseMode.php` script to ensure your Tenable Security Center Director databases are fully converted to WAL journaling mode.

WAL Requirements

Note: Write-ahead logging mode typically uses more disk space than DELETE mode. Consider your disk space availability before enabling write-ahead logging. Tenable recommends the same amount of disk space that is occupied by the database.

In addition to the requirements to run Tenable Security Center Director, your Tenable Security Center Director installation must be running Tenable Security Center Director 5.19.x or later.

Databases Affected

Enabling or disabling WAL converts the database journaling mode for the following Tenable Security Center Director databases:

- `/opt/sc/application.db`
- `/opt/sc/hosts.db`
- `/opt/sc/jobqueue.db`
- `/opt/sc/plugins.db`
- `/opt/sc/remediationHierarchy.db`
- `/opt/sc/orgs/<orgID>/organization.db` (for each organization in your Tenable Security Center Director)
- `/opt/sc/orgs/<orgID>/assets.db` (for each organization in your Tenable Security Center Director)

The `convertDatabaseMode.php` script only converts the database journaling mode for Tenable Security Center Director databases that can significantly impact performance.

Enable Write-Ahead Logging

Required Tenable Security Center User Role: Root user

Note: This topic assumes a basic understanding of Linux.

You can use the `convertDatabaseMode.php` script to enable write-ahead logging (WAL) journaling mode for Tenable Security Center Director databases. Enabling WAL may resolve issues with excessive database locks. If your Tenable Security Center Director does not experience database locking issues, Tenable recommends leaving your Tenable Security Center Director databases in the default DELETE journaling mode.

For more information, see Tenable Security Center Director Database Journaling Modes.

Before you begin:

- Confirm your Tenable Security Center Director installation meets the requirements to enable WAL. For more information, see WAL Requirements.
- Write-ahead logging mode typically uses more disk space than DELETE mode. Consider your disk space availability before enabling write-ahead logging. Tenable recommends the same amount of disk space that is occupied by the database.
- Perform a backup of Tenable Security Center Director, as described in Perform a Backup.

To enable WAL:

1. Log in to Tenable Security Center Director via the command line interface (CLI).
2. Stop Tenable Security Center Director, as described in Start, Stop, or Restart Tenable Security Center Director.
3. In the CLI in Tenable Security Center Director, run the following command to start the `converDatabaseMode.php` script:

   ```
   /opt/sc/support/bin/php /opt/sc/src/tools/convertDatabaseMode.php -m WAL
   ```

   The script runs.
4. If the script detects any running `tns` user processes, repeat the following steps for each `tns` user process detected:
   a. Follow the prompts in the error output to halt the `tns` user process.

      Example error output:

      ```
      Error! The Tenable Security Center process with PID '10135' is still running
      and needs to be halted before this script can be executed successfully.
         Command: /opt/sc/support/bin/php -f /opt/sc/daemons/Jobd.php
      Bailing with 146.
      ```

   b. Run the following command to restart the `converDatabaseMode.php` script:

```
/opt/sc/support/bin/php /opt/sc/src/tools/convertDatabaseMode.php -m WAL
```

The script restarts.

Tenable Security Center Director converts supported databases to WAL journaling mode. For more information, see Databases Affected.

5. Start Tenable Security Center Director, as described in Start, Stop, or Restart Tenable Security Center Director.

What to do next:

- Perform regular backups of Tenable Security Center Director, as described in Perform a Backup.

Disable Write-Ahead Logging

Required Tenable Security Center User Role: Root user

Note: This topic assumes a basic understanding of Linux.

If you experience issues with write-ahead logging (WAL), disable WAL by reverting your Tenable Security Center Director databases to DELETE journaling mode. For more information, see Tenable Security Center Director Database Journaling Modes.

Before you begin:

- Perform a backup of Tenable Security Center Director, as described in Perform a Backup.

To disable WAL:

1. Log in to Tenable Security Center Director via the command line interface (CLI).
2. Stop Tenable Security Center Director, as described in Start, Stop, or Restart Tenable Security Center Director.
3. In the CLI in Tenable Security Center Director, run the following command to start the `converDatabaseMode.php` script:

```
/opt/sc/support/bin/php /opt/sc/src/tools/convertDatabaseMode.php -m DELETE
```

The script runs.

4. If the script detects any running `tns` user processes, repeat the following steps for each `tns` user process detected:

   a. Follow the prompts in the error output to halt the `tns` user process.

   Example error output:

   ```
   Error! The Tenable Security Center process with PID '10135' is still running
   and needs to be halted before this script can be executed successfully.
      Command: /opt/sc/support/bin/php -f /opt/sc/daemons/Jobd.php
   Bailing with 146.
   ```

   b. Run the following command to restart the `converDatabaseMode.php` script:

   ```
   /opt/sc/support/bin/php /opt/sc/src/tools/convertDatabaseMode.php -m DELETE
   ```

   The script restarts.

   Tenable Security Center Director converts supported databases to DELETE journaling mode. For more information, see Databases Affected.

5. Start Tenable Security Center Director, as described in Start, Stop, or Restart Tenable Security Center Director.

What to do next:

- Perform regular backups of Tenable Security Center Director, as described in Perform a Backup.

License Requirements

This topic breaks down the licensing process for Tenable Security Center as a standalone product. It also explains how assets are counted, lists add-on components you can purchase, and describes

what happens during license overages or expiration.

Important! To purchase Tenable products, contact your Tenable Representative.

Tenable Security Center Versions

Tenable Security Center has two versions:

- **Tenable Security Center** – Includes Tenable Network Monitor in discovery mode and unlimited Tenable Nessus scanners.
- **Tenable Security Center+** – Includes all of the above plus Tenable Network Monitor with vulnerability detection and metrics such as Asset Exposure Score (AES) and Asset Criticality Rating (ACR).

Tenable Security Center Director is available for both versions. Tenable Security Center Director is an add-on with which you can manage multiple Tenable Security Center instances from one location. For more information, see the Tenable Security Center Director User Guide.

Note: You cannot upgrade a Tenable Security Center license to a Tenable Security Center Director license or downgrade a Tenable Tenable Security Center Director license to a Tenable Security Center license.

Licensing Tenable Security Center

To use any version of Tenable Security Center, you purchase licenses based on your organizational needs and environmental details. Tenable Security Center assigns those licenses to your *assets*, which are hosts assessed for vulnerabilities or imported from other Tenable products.

Note: Tenable offers simplified pricing to managed security service providers (MSSPs). To learn more, contact your Tenable representative.

How Assets are Counted

Tenable Security Center licenses are valid for specific hosts and a maximum number of active assets identified by IP address or UUID. Assets count towards your license depending on how Tenable Security Center discovers them. In general, assets do not count unless they have been assessed for vulnerabilities.

For example, if you purchase a 500 asset 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 in the *Tenable Security Center User Guide*.

The following table explains when assets count towards your license.

Counted Towards Your License	Not Counted Towards Your License
• Assets from active scans. • Assets from Tenable Network Monitor instances not in discovery mode. • Assets in offline or remote repositories that you downloaded using the same Tenable Security Center instance or license. **Note**: In agent or IPv4 repositories, each single IP address or UUID counts once toward your license, even if it was scanned via multiple methods or stored in multiple repositories. In universal repositories, each asset with a UUID is counted toward your license. For example, if an asset in an IPv4 repository does not have a UUID, and the same asset is stored in a universal repository with a UUID, the asset is counted twice. **Note**: If you use an alternative port scanner, Tenable Security Center counts the detected IP addresses against your license.	• Assets present only from imports to offline or remote repositories. • Assets present only from Tenable Network Monitor instances in discovery mode. • Assets in offline or remote repositories that you downloaded using the same Tenable Security Center instance with a different license. • Assets in offline or remote repositories that you downloaded using a different Tenable Security Center instance and license. • In the latest versions of Tenable Security Center and Tenable Security Center Director, the following excluded plugins:

Counted Towards Your License	Not Counted Towards Your License
	Tenable Nessus – 10180, 10287, 10335, 11219, 11933, 11936, 12053, 14272, 14274, 19506, 22964, 33812, 33813, 34220, 34277, 45590, 54615, 87413, 112154, 161455, 179042, 209654, and 204872. **Tenable Network Monitor** – 0, 12, 18, 19, 20, 113, and 132.

Note: In the context of this table, assets are differentiated by the type of repository the data is stored in. For example:

- in IPv4 and IPv6 repositories, *assets* are *IP addresses*.
- in agent repositories, *assets* are *agents*.
- in universal repositories, *assets* are *hosts*.

For more information, see Asset Tracking in Tenable Security Center.

Tenable Security Center Components

You can customize Tenable Security Center for your use case by adding components. Some components are add-ons that you purchase.

Version	Included with Purchase	Add-on Component
Tenable Security Center	• One console (or more with additional IP addresses). • Tenable Network	• Cloud Tenable Agents. • Tenable Network Monitors in high-performance mode. • (Subscription-only) Additional consoles. • (Subscription-only) Security Center Lab

	Monitor in discovery mode. • Tenable Nessus scanners. • Vulnerability Probability Rating (VPR). • (Subscription-only) The same number of on-premises Tenable Agents as your licensed assets, provided on request.	License. • Tenable One Web App Scanning, to scan web applications with a Tenable Nessus scanner in Tenable Security Center. Scan up to your number of licensed fully qualified domain names (FQDNs). For more information, see Web App Scans in the *Tenable Security Center User Guide*. **Note**: If you already have a Tenable Security Center license and you upgrade to Tenable Security Center version 6.2.x or later, there are two ways to enable web application scans. Either update your Tenable One Web App Scanning plugins manually in Tenable Security Center or wait for the nightly plugin update to run. • (Subscription-only) Tenable Security Center Director. • (Perpetual-only) On-Premises Tenable Agents, which Perpetual customers must purchase separately. • Tenable One Attack Surface Management. • Vulnerability Intelligence. **Note:** Vulnerability Intelligence is included with all Subscription licenses, and available as an add-on for Perpetual licenses.
Tenable Security Center+	• One console (or more with additional IP addresses).	• Cloud Tenable Agents. • Tenable Network Monitors in high-performance mode.

	• Tenable Network Monitor in discovery mode. • Tenable Network Monitors with vulnerability detection. • Tenable Nessus scanners. • Asset Exposure Score (AES). • Vulnerability Priority Rating (VPR). • (Subscription-only) The same number of on-premises Tenable Agents as your licensed assets, provided on request.	• (Subscription-only) Additional consoles. • (Subscription-only) Security Center Lab License. • Tenable One Web App Scanning, to scan web applications with a Tenable Nessus scanner in Tenable Security Center. Scan up to your number of licensed fully qualified domain names (FQDNs). For more information, see Web App Scans in the *Tenable Security Center User Guide*. **Note**: If you already have a Tenable Security Center license and you upgrade to Tenable Security Center version 6.2.x or later, there are two ways to enable web application scans. Either update your Tenable One Web App Scanning plugins manually in Tenable Security Center or wait for the nightly plugin update to run. • (Subscription-only) Tenable Security Center Director. • (Perpetual-only) On-Premises Tenable Agents, which Perpetual customers must purchase separately. • Tenable One Attack Surface Management. • Vulnerability Intelligence. **Note:** Vulnerability Intelligence is included with all Subscription licenses, and available as an add-on for Perpetual licenses.

Reclaiming Licenses

Tenable Security Center's license count updates when you delete a repository, run a license report, or upload a new license. If you set assets to age out, they are removed during nightly cleanup. If you configure your scan settings to remove unresponsive hosts, they are removed at scan import.

For more information, see License Count in the *Tenable Security Center Best Practices Guide*.

Exceeding the License Limit

As you approach or exceed your license limit, a warning appears in the Tenable Security Center interface. If you exceed your limit, Tenable disables your access to Tenable Security Center. To upgrade your license, contact your Tenable representative.

Expired Licenses

The Tenable Security Center licenses you purchase are valid for the length of your contract. 30 days before your license expires, a warning appears in the user interface. During this renewal period, work with your Tenable representative to add or remove products or change your license count.

After your license expires, your Tenable products and components are affected as follows:

- **Tenable Security Center Console (Perpetual license)** – The software remains fully functional. All user data is accessible.
- **Tenable Security Center Console (Subscription license)** – To access the console, you must enter a new license key. Once you enter a new license key, normal operation resumes.
- **Tenable Nessus (Perpetual license)** – When your maintenance period expires, plugin updates are no longer available. After 90 days, Tenable Nessus stops working and you cannot perform new scans. Because Tenable Security Center stops receiving feeds, the Tenable Nessus scanners managed by your managed Tenable Security Center instances no longer receive updates and also stop working.
- **Tenable Network Monitor (Perpetual license)** – After 30 days with no updates, new data is no longer processed.

License Statuses

Tenable Security Center uses a platform licensing service to manage and report the license state. The following table describes the statuses you may see in the Tenable Security Center user interface or licensing API.

The following table describes the possible statuses for your overall Tenable Security Center license.

Status	Description
Valid	The license is within its expiration date and all licensed blades are operational.
Exceeded	You have exceeded your licensed asset count. Tenable Security Center generates a warning in the user interface. If the overage continues, functionality is progressively reduced. For more information, see Exceeding the License Limit.
Locked	The license enforcement ID (cluster ID or namespace ID) does not match the current deployment. No blades are accessible until the license is re-applied with the correct ID.
Expired	The license expiration date has passed. You can no longer sign in to Tenable Security Center. Contact your Tenable representative to renew.

Working with License Keys

The following sections explain how to work with Tenable license keys and link to additional details.

Get a Tenable Security Center License Key

To get a Tenable Security Center license key, see Download License Key in the *Tenable Account Management* documentation.

> **Tip**: To obtain the hostname of your installation machine, in a system shell prompt, type `hostname`. You can also use the install UUID in place of the hostname. The install UUID appears on the license activation page of the initial setup wizard, and is also available in the install log and in the `install-uuid.txt` file.

Get an Activation Code for an Attached Product

Activation codes are required for Tenable products attached to Tenable Security Center, such as Tenable Nessus. To get an activation code, see Product Details in the *Tenable Account Management* documentation.

Add or Update a Tenable Security Center License Key

In most cases, adding a license key to Tenable Security Center or its attached products requires the Tenable Security Center console to contact a product registration server. The server connection is encrypted, as described in Encryption Strength.

Tip: To learn which Tenable sites to allow through your firewall, see the Tenable Knowledge Base.

Note: For instructions to use in offline or air-gapped environments, see Offline Plugin and Feed Updates for Tenable Security Center.

See the following topics for instructions to upload a new license key or update an existing one:

- Quick Setup – Upload a new Tenable Security Center license and add activation codes for any attached products.
- Apply a New License – Upload a new license for attached Tenable products only.
- Update an Existing License – Update an existing Tenable Security Center license or existing attached Tenable product licenses.

Apply a New License

Required Tenable Security Center 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 download Tenable Security Center, see the Tenable Security Center downloads page.

Caution: Do not open the license key file in a text editor. Opening the file in a text editor can corrupt it and prevent Tenable Security Center from accepting the license.

To apply a new Tenable Nessus or Tenable Network Monitor license:

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, 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.

   Note: To locate your activation code, log in to your Tenable account at https://account.tenable.com/products/purchased and find the activation code for your product.
6. Click **Register**.

   Tenable Security Center 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 Security Center initiates a plugin download.

Update an Existing License

Required Tenable Security Center User Role: Administrator

Tip: Tenable rebranded Tenable Security Center Continuous View as Tenable Security Center+.

If you need to replace your Tenable Security Center Director license or the license activation code for your Tenable Nessus or Tenable Network Monitor license, update the license.

To apply a new license for another Tenable product for the first time, see Apply a New License.

You can update your Tenable Security Center Director license in an externally connected or air-gapped environment. Tenable Security Center Director requires an internet connection to validate product licenses for Tenable Nessus or Tenable Network Monitor.

For instructions on how to install a Tenable Security Center patch, see Install a Patch.

To download Tenable Security Center, see the Tenable Security Center Downloads page.

For general information about licensing, see License Requirements.

Caution: Do not open the license key file in a text editor. Opening the file in a text editor can corrupt it and prevent Tenable Security Center from accepting the license.

To update a license:

1. Download the new license key:
    a. Log in to your Tenable account at https://account.tenable.com/products/purchased.
    b. Locate your Tenable Security Center Director product and click **Set Hostname** to register your instance.
    c. Click **Download License Key** to download the `.key` license file to your computer.
2. Log in to Tenable Security Center Director through the user interface.
3. Click **System** > **Configuration**.

    The **Configuration** page appears.
4. Click the **License** tile.

    The **License Configuration** page appears.

    Note: If you do not see the **License** tile, verify that your user account has the Administrator role.
5. To replace your Tenable Security Center Director license, in the **Tenable Security Center Director License** section:

a. Click **Update License**.

b. Click **Choose File** and browse to the license file you want to upload.

Tenable Security Center Director applies the new license.

6. 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.

> **Note:** To locate your activation code, log in to your Tenable account at https://account.tenable.com/products/purchased and find the activation code for your product.

d. Click **Register**.

Tenable Security Center Director communicates with the Tenable product registration server to validate your license activation code.

If the code is valid, Tenable Security Center Director applies the new license and initiates a plugin download.

Port Requirements

Tenable Security Center port requirements include Tenable Security Center-specific, Tenable Security Center Director-specific, and application-specific requirements.

Tenable Security Center Instance

Your Tenable Security Center instances require access to specific ports for inbound and outbound traffic.

Inbound Traffic

You must allow inbound traffic to the following ports.

Port	Traffic
TCP 22	Performing remote repository synchronization with another Tenable Security Center.
TCP 443	Accessing the Tenable Security Center interface. Communicating with Tenable Security Center Director instances. Communicating with Tenable One OT Exposure instances. Performing the initial key push for remote repository synchronization with another Tenable Security Center. Interacting with the API.
TCP 8837	Communicating with linked scans.

Note: Tenable Security Center reserves TCP 5432 for the PostgreSQL database that Tenable Security Center manages. If you install a custom PostgreSQL database on the same host as Tenable Security Center, do not use port 5432, because Tenable Security Center assumes that port belongs to the managed database.

Outbound Traffic

You must allow outbound traffic to the following ports.

Port	Traffic
TCP 22	Synchronizing repositories from other Tenable Security Center instances.
TCP 25	Sending SMTP email notifications.
TCP 389	Communicating with customer-managed LDAP servers.
TCP 443	Communicating with Tenable One for synchronization.

Port	Traffic
	Communicating with the `plugins.nessus.org` server for plugin updates.
TCP 465	Sending SMTP email notifications.
TCP 587	Sending SMTP email notifications.
TCP 636	Communicating with customer-managed LDAP servers.
TCP 8834	Communicating with Tenable Nessus.
TCP 8835	Communicating with Tenable Network Monitor.
UDP 53	Performing DNS resolution.

Note: If your Tenable Security Center instance is not configured as an offline instance, you must also allow outbound traffic to the Tenable websites listed in the Which Tenable sites should I allow? article in the Knowledge Base.

SSL inspection on traffic to and from the Tenable update sites is not supported. While access to the update sites can be established, it may not be able to complete updates due to SSL inspection of the traffic.

Tenable Security Center Services

The following are reserved ports for Tenable Security Center services.

Port	Traffic
TCP 8840	Tenable Security Center asset service.
TCP 8841	Tenable Security Center finding service.

Tenable Security Center Director

Your Tenable Security Center Director instances require access to specific ports for inbound and outbound traffic.

Inbound Traffic

You must allow inbound traffic to the following ports.

Port	Traffic
TCP 22	Performing remote repository synchronization with another Tenable Security Center.
TCP 443	Accessing the Tenable Security Center Director interface. Communicating with managed Tenable Security Center instances. Accessing the Tenable Security Center API interface. Performing automatic SSH key setup to synchronize remote repositories with another Tenable Security Center.

Outbound Traffic

You must allow outbound traffic to the following ports.

Port	Traffic
TCP 25	Sending SMTP email notifications.
TCP 443	Communicating with the `plugins.nessus.org` server for plugin updates. Performing automatic SSH key setup to synchronize remote repositories with another Tenable Security Center.
TCP 465	Sending SMTP email notifications.

Port	Traffic
TCP 587	Sending SMTP email notifications.
UDP 53	Performing DNS resolution.

Note: If your Tenable Security Center Director instance is not configured as an offline instance, you must also allow outbound traffic to the Tenable websites listed in the Which Tenable sites should I allow? article in the Knowledge Base.

SSL inspection on traffic to and from the Tenable update sites is not supported. While access to the update sites can be established, it may not be able to complete updates due to SSL inspection of the traffic.

Tenable Nessus Scanner

Your Tenable Nessus instances require access to specific ports for inbound and outbound traffic.

Inbound Traffic

You must allow inbound traffic to the following ports.

Port	Traffic
TCP 8834	Accessing the Tenable Nessus interface. Communicating with Tenable Security Center. Interacting with the API.

Outbound Traffic

You must allow outbound traffic to the following ports.

Port	Traffic
TCP 25	Sending SMTP email notifications.
TCP 443	Communicating with Tenable One Vulnerability Management (sensor.cloud.tenable.com or sensor.cloud.tenablecloud.cn). Communicating with the `plugins.nessus.org` server for plugin updates.
UDP 53	Performing DNS resolution.

Tenable Agent

Your Tenable Agents require access to specific ports for outbound traffic.

Outbound Traffic

You must allow outbound traffic to the following ports.

Port	Traffic
TCP 443	Communicating with Tenable One Vulnerability Management.
TCP 8834	Communicating with Tenable Nessus Manager. **Note:** The default Tenable Nessus Manager port is TCP 8834. However, this port is configurable and may be different for your organization.
UDP 53	External DNS support for the host that Tenable Agent is installed on. Several plugins use DNS resolution in their operation.

Note: Operating system installation commands, such as `dnf install`, may require other connections besides Tenable One Vulnerability Management or Tenable Nessus Manager. Consult your operating system administrator for more information.

Tenable Network Monitor

Your Tenable Network Monitor instances require access to specific ports for inbound and outbound traffic.

Inbound Traffic

You must allow inbound traffic to the following ports.

Port	Traffic
TCP 8835	Accessing the Tenable Network Monitor interface. Communicating with Tenable Security Center.

Outbound Traffic

You must allow outbound traffic to the following ports.

Port	Traffic
TCP 443	Communicating with Tenable One Vulnerability Management (sensor.cloud.tenable.com or sensor.cloud.tenablecloud.cn). Communicating with the `plugins.nessus.org` server for plugin updates.
TCP 601	Communications for reliable TCP syslog forwarding.
UDP 53	Performing DNS resolution.
UDP 514	Communications for UDP syslog forwarding.

Browser Requirements

Note: Tenable recommends using the newest available version of your browser.

Note: Tenable Security Center Director does not officially support any browser extensions. If you encounter issues related to browser extensions, please report them to the relevant browser extension developer for further assistance.

You can access the Tenable Security Center Director user interface using the following browsers:

- Mozilla Firefox 87 or later
- Google Chrome 89 or later
- Mac OS Safari 14.02 or later
- Microsoft Edge 99 or later

Tenable Integrated Product Compatibility

The versions of Tenable products tested with Tenable Security Center Director 6.10.x are available in the release notes. For more information, see the Tenable Security Center Release Notes for your version.

Tenable Security Center Director Version	Product	Tested Version
6.8.x	Tenable Nessus	10.8.0 and later
	Tenable One OT Exposure	3.19.0 and later
	Tenable Network Monitor	6.5.0 and later
6.7.x	Tenable Nessus	10.5.0 and later
	Tenable One OT Exposure	3.16.0 and later
	Tenable Network Monitor	6.2.0 and later

Tenable Security Center Director Version	Product	Tested Version
6.6.x	Tenable Nessus	8.9.0 and later
	Tenable One OT Exposure	3.9.25 and later
	Tenable Network Monitor	5.11.0 and later
6.5.x	Tenable Nessus	8.9.0 and later
	Tenable One OT Exposure	3.9.25 and later
	Tenable Network Monitor	5.11.0 and later
6.2.x	Tenable Nessus	8.9.0 and later
	Tenable One OT Exposure	3.9.25 and later
	Tenable Network Monitor	5.11.0 and later

Large Enterprise Deployments

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

External PostgreSQL with Tenable Security Center Director

Note: When reviewing external PostgreSQL documentation, ensure that you use the appropriate documentation version for the PostgreSQL version you deployed.

For information about using the managed PostgreSQL server in Tenable Security Center Director, see Using the Managed PostgreSQL Server.

Requirements

If your Tenable Security Center Director installation manages more than 100,000 assets, Tenable strongly recommends that you use an external PostgreSQL server for performance. Depending on deployment complexity or usage, Tenable Support may recommend that you use an external PostgreSQL server for improved performance, even if you manage fewer than 100,000 assets.

Note: If you migrate from a Tenable Security Center on-premises deployment to a Tenable Enclave Security deployment, you must use an external PostgreSQL server. Before you migrate, the Tenable Security Center on-premises deployment must use the same external PostgreSQL server that you plan to use after the migration.

Migration Between Internal and External PostgreSQL

You can use the Tenable-provided script and instructions to migrate between an internal and external PostgreSQL implementations with Tenable Security Center Director.

Responsibility Matrix

You are responsible for the following when you use an external PostgreSQL server with Tenable Security Center Director:

- Installing and configuring PostgreSQL
- Backing up PostgreSQL
- Securing PostgreSQL
- Patching and upgrading PostgreSQL

Tenable is responsible for:

- The Tenable Security Center Director database and structure within PostgreSQL
- Data integrity and database-level configuration

You must not access or modify the Tenable Security Center Director database within PostgreSQL directly.

Installation

You may use any currently supported version of PostgreSQL. These include:

- PostgreSQL 13.x
- PostgreSQL 14.x
- PostgreSQL 15.x
- PostgreSQL 16.x (preferred)
- PostgreSQL 17.x

Tenable follows the PostgreSQL lifecycle and removes support after that major version's final version is released. For example, Tenable will not support PostgreSQL 13.x after November 2025.

Caution: If you use an external PostgreSQL 17, Tenable does not currently support migrating back to an internal PostgreSQL database.

Follow the PostgreSQL documentation for installation instructions.

You may choose a managed (by a cloud vendor or other) instance of PostgreSQL, as long as you meet the requirements listed above.

Note: When you use an external PostgreSQL database and you uninstall Tenable Security Center Director, the associated PostgreSQL database remains. Contact your Database Administrator to remove the database properly and completely, and ensure you take and maintain any required backups.

Configuration

External PostgreSQL Resource Requirements

For hardware requirements for PostgreSQL with Tenable Security Center Director, see Hardware Requirements

The table below shows the sizing requirements for Tenable Security Center Director based on the asset count. Tenable uses this information to determine the appropriate PostgreSQL configuration parameters needed for optimal Tenable Security Center Director performance.

You can set PostgreSQL configuration items using various methods. Review the PostgreSQL documentation for information on how to apply these configuration changes.

The following are recommended settings for various Tenable Security Center Director sizes:

> 4 vCPUs/16 GB RAM, Cloud Equivalent- m6g.xlarge (2,500 active IPs and ~2 million Vulnerabilities)

```
max_connections=50
max_worker_processes=4
max_parallel_workers_per_gather=2
max_parallel_maintenance_workers=2
max_parallel_workers=4
shared_buffers=4GB
work_mem=128MB
maintenance_work_mem=1024MB
effective_cache_size=12GB
default_statistics_target=100
checkpoint_completion_target=0.9
wal_buffers=128MB
max_wal_size=6GB
min_wal_size=3GB
checkpoint_timeout=15min
wal_writer_flush_after=4MB
```

```
wal_writer_delay=10ms
effective_io_concurrency=200
random_page_cost=1.1
```

8 vCPUs/32 GB RAM, Cloud Equivalent- m6g.2x large (10,000 active IPs and ~8 million Vulnerabilities)

```
max_connections=50
max_worker_processes=8
max_parallel_workers_per_gather=4
max_parallel_maintenance_workers=4
max_parallel_workers=8
shared_buffers=8GB
work_mem=256MB
maintenance_work_mem=2048MB
effective_cache_size=24GB
default_statistics_target=100
checkpoint_completion_target=0.9
wal_buffers=128MB
max_wal_size=8GB
min_wal_size=4GB
checkpoint_timeout=15min
wal_writer_flush_after=4MB
wal_writer_delay=10ms
effective_io_concurrency=200
random_page_cost=1.1
```

16 vCPUs/64 GB RAM, Cloud Equivalent- m6g.4x large (25,000 active IPs)

```
max_connections=50
max_worker_processes=16
max_parallel_workers_per_gather=4
max_parallel_maintenance_workers=4
```

```
max_parallel_workers=16
shared_buffers=16GB
work_mem=512MB
maintenance_work_mem=2048MB
effective_cache_size=48GB
default_statistics_target=100
checkpoint_completion_target=0.9
wal_buffers=128MB
max_wal_size=12GB
min_wal_size=6GB
checkpoint_timeout=15min
wal_writer_flush_after=4MB
wal_writer_delay=10ms
effective_io_concurrency=200
random_page_cost=1.1
```

32 vCPUs/128 GB RAM, Cloud Equivalent- m6g.8x large (70,000 Hosts and ~40 million Vulnerabilities)

```
max_connections=50
max_worker_processes=32
max_parallel_workers_per_gather=4
max_parallel_maintenance_workers=4
max_parallel_workers=32
shared_buffers=32GB
work_mem=1024MB
maintenance_work_mem=2048MB
effective_cache_size=96GB
default_statistics_target=100
checkpoint_completion_target=0.9
wal_buffers=128MB
max_wal_size=20GB
min_wal_size=10GB
checkpoint_timeout=15min
```

```
wal_writer_flush_after=4MB
wal_writer_delay=10ms
effective_io_concurrency=200
random_page_cost=1.1
```

64 vCPUs/256 GB RAM, Cloud Equivalent- m6g.16x large

```
max_connections=50
max_worker_processes=64
max_parallel_workers_per_gather=4
max_parallel_maintenance_workers=4
max_parallel_workers=64
shared_buffers=64GB
work_mem=1024MB
maintenance_work_mem=2048MB
effective_cache_size=192GB
default_statistics_target=100
checkpoint_completion_target=0.9
wal_buffers=128MB
max_wal_size=24GB
min_wal_size=12GB
checkpoint_timeout=20min
wal_writer_flush_after=4MB
wal_writer_delay=10ms
effective_io_concurrency=200
random_page_cost=1.1
```

Enable Slow Query Data for the Diagnostics Bundle

To include slow query data in the diagnostics bundle, you must explicitly enable the `pg_stat_statements` module on the PostgreSQL database that you configured for Tenable Security Center Director.

1. As a PostgreSQL superuser, add `pg_stat_statements` to `shared_preload_libraries`:

   ```
   psql -c "ALTER SYSTEM SET shared_preload_libraries = 'pg_stat_statements';"
   ```

   If other libraries are already loaded (for example, `pgaudit` and `pgcrypto`), append `pg_stat_statements` to the existing list instead:

   ```
   psql -c "ALTER SYSTEM SET shared_preload_libraries = 'pgaudit,pgcrypto,pg_stat_statements';"
   ```

2. Restart PostgreSQL:

   ```
   systemctl restart postgresql
   ```

   Alternatively, run `pg_ctl restart -D` *<path to data directory>*.

3. Create the extension in the Tenable Security Center Director database:

   ```
   psql -d {SC_DB} -c "CREATE EXTENSION IF NOT EXISTS pg_stat_statements;"
   ```

   Replace `{SC_DB}` with the name of your Tenable Security Center Director database.

4. Verify the configuration:

   ```
   psql -c "SHOW shared_preload_libraries;"
   ```

   ```
   psql -d {SC_DB} -c "SELECT * FROM pg_stat_statements LIMIT 1;"
   ```

Security

Tenable recommends that you implement an applicable PostgreSQL security baseline–such as the Center for Internet Security (CIS) PostgreSQL Benchmark or the Crunchy Data PostgreSQL STIG–if you host your own PostgreSQL instance. Tenable does not provide support for implementing these

benchmarks, and some configurations may impact Tenable Security Center Director performance or functionality.

Implementation of security benchmarks may require adding external extensions, for example, `pgaudit` and `pgcrypto`, to PostgreSQL. Tenable does not provide support or documentation on how to install or configure these extensions.

External PostgreSQL Credential Encryption

You can encrypt on-disk usernames and passwords for your external PostgreSQL credentials.

By default, PostgreSQL usernames and passwords are stored in plain text in the `/opt/sc/.pgvars` file. After installation, you can use the Tenable Security Center Director encryption utility to encrypt these credentials and update the `.pgvars` file.

Tenable Security Center Encryption Utility Overview (sc-enc)

The encryption utility binary is located at: `/opt/sc/bin/sc-enc-linux-amd64`.

```
NAME:
    sc-enc - A Command Line Interface (CLI) tool for Advanced Encryption Standard (AES)
encryption

USAGE:
    sc-enc [global options] command [command options]

VERSION:
    1.0.0

COMMANDS:
    encrypt      Encrypts a string using AES encryption
    decrypt      Decrypts a string using AES encryption
    generate     Generates a key
    grpc-server  Starts a gRPC server for encryption and decryption
    help, h      Shows a list of commands or help for one command
```

```
GLOBAL OPTIONS:
    --key-path value, -k value  Specifieds the encryption key (default:
"/opt/sc/data/enc.key")
    --fips-disable, --fd        Disables Federal Information Processing Standards
(FIPS) 140-2 mode (default: false)
    --help, -h                  Shows help information
    --version, -v               Prints the version
```

To encrypt external PostgreSQL credentials after installation:

Note: The sc-enc utility must be run as the `tns` user on the Tenable Security Center Director server where the credentials will be used. Tenable Security Center Director generates the encryption key (`/opt/sc/data/enc.key`) during installation, and the key is unique to that server. Encrypted credentials generated on one Tenable Security Center Director server cannot be used on a different server.

1. Install Tenable Security Center Director with non-encrypted PostgreSQL credentials in the `.pgvars` file.
2. (Optional) After installation, update your PostgreSQL server credentials.
3. Stop Tenable Security Center Director.

   ```
   # /bin/systemctl stop SecurityCenter
   ```

4. Switch to the `tns` user:

   ```
   su - tns
   ```

5. Run the sc-enc utility with the `encrypt` command to encrypt the PostgreSQL username and password. The following is an example, where `[value]` is the username or password you want to encrypt.

   ```
   /opt/sc/bin/sc-enc-linux-amd64 encrypt -i [value]
   ```

The output produces the encrypted string:

```
sc_enc:1:c05eab151b29704f133dd597552d7ca1f11ba34fb25716fb9e62f2c1f6073df7
```

6. Update the `.pgvars` file with the encrypted values.

```
export SC_PG_HOST=127.0.0.1
export SC_PG_PORT=5432
export SC_PG_USER=sc_
enc:1:c05eab151b29704f133dd597552d7ca1f11ba34fb25716fb9e62f2c1f6073df7
export SC_PG_PASSWORD=sc_
enc:1:2c80aaf0a140443abdf1820f9a8dd78ea0caf4fe234dd0ba43713e09d048cb8c
export SC_PG_DATABASE=SecurityCenter
export SC_PG_CA_PATH=
export SC_PG_REQUIRE_TLS=
```

7. Start Tenable Security Center Director.

Note: Tenable Security Center Director automatically generates an encryption key during installation or upgrade. The key is stored at `/opt/sc/data/enc.key`. Tenable recommends that you back up this key and store it in a safe location.

Patching and Upgrades

Note: You must shut down Tenable Security Center Director before you patch or upgrade PostgreSQL.

Tenable recommends you do the following:

- Monitor PostgreSQL Security Updates and apply the relevant security patches after testing.
- Take a backup of the Tenable Security Center Director database before you patch or upgrade PostgreSQL.

Connect an External PostgreSQL Server

You must configure an external PostgreSQL database if your Tenable Security Center Director installation meets any of the following criteria:

- Your Tenable Security Center Director instance has over 100,000 assets.
- Your Tenable Security Center Director instance is a non-rpm installation.
- You are migrating from a Tenable Security Center Director on-prem installation to a Security Center on Tenable Enclave Security installation. You must configure the external PostgreSQL server for your on-prem Tenable Security Center Director before migration, and the Tenable Enclave Security installation must use the same external PostgreSQL server.

Note: Tenable Security Center Director does not support multiple Tenable Security Center Director instances using the same database name in the same PostgreSQL server. The database name should be unique in the PostgreSQL instance.

Note: Tenable Security Center Director supports PostgreSQL versions 13.x through 17.x.

For information about how to configure a PostgreSQL server, see the PostgreSQL documentation.

For sizing recommendations, see the Hardware Requirements and Cloud Requirements.

To connect your Tenable Security Center Director instance to your PostgreSQL server:

1. Before you install or upgrade Tenable Security Center Director, populate the following environment variables:

   Note: For a fresh install, you must set the environment variables with a `root` user account. If you are upgrading a previous installation with new PostgreSQL values, you must modify the values in the `/opt/sc/.pgvars` file. The values in the `.pgvars` file will be the source for connecting to the defined PostgreSQL server.

   - `SC_PG_HOST` (required)- The IP address or hostname of the external PostgreSQL server.
   - `SC_PG_USER` (required) - The PostgreSQL username.

     Note: The PostgreSQL user account must have CREATEDB and read/write permissions.

   - `SC_PG_PORT` (required) - The port number. The default port is **5432**.

- `SC_PG_PASSWORD` - The password for the PostgreSQL user. If you do not provide a password, Tenable Security Center Director will assume an empty password for the external PostgreSQL user.
- `SC_PG_DATABASE` (required) - The database name for the Tenable Security Center Director data. The default database name is **SecurityCenter**.
- `SC_PG_CA_PATH` - The absolute path to the cert file. When you specify the location of the root certificate, Tenable Security Center Director verifies the root certificate used by PostgreSQL.
- `SC_PG_REQUIRE_TLS` - Whether PostgreSQL uses SSL. If this variable is not set, `ssl_mode` defaults to `prefer`. Valid values: `require`, `prefer`, `verify-ca`, `verify-full`.

After you install or upgrade to Tenable Security Center Director 6.5.0 or later, then Tenable Security Center Director will attempt to connect to the PostgreSQL instance using the values provided and create a database with the specified database name.

Backup and Restore Tenable Security Center Director with an External PostgreSQL

For more information about PostgreSQL with Tenable Security Center Director, see External PostgreSQL with Tenable Security Center Director.

Before you Begin

- Tenable recommends either a SQL Dump or a File System Level Backup for simplicity.
- Review the PostgreSQL documentation on backups and restores.

Backup and Restore Tenable Security Center Director with an External PostgreSQL database:

1. Stop Tenable Security Center Director.
2. Back up PostgreSQL according to the PostgreSQL documentation.
3. Back up the Tenable Security Center Director application.

4. Restore PostgreSQL according to the PostgreSQL documentation, and ensure the connection details are the same.
5. Install the Tenable Security Center Director RPM matching the backup version and architecture if needed.
6. Restore Tenable Security Center from the backup file you created in step 3.

Installation and Upgrade

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

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

To uninstall Tenable Security Center Director, see Uninstall Tenable Security Center Director.

Before You Install

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

Check System Requirements

Before you begin the installation, ensure that the target system meets the hardware and software requirements for your specific deployment size. Failure to meet these requirements can lead to performance degradation or installation failure.

For more information, see Requirements.

Understand Tenable Security Center and Tenable Security Center Director Licenses

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

For more information, see License Requirements.

Plan Your Tenable Security Center Director Deployment Version

You must run the same version of Tenable Security Center on your entire Tenable Security Center Director deployment, including Tenable Security Center Director and all managed Tenable Security Center instances that you connect to Tenable Security Center Director. Tenable Security Center Director cannot communicate with managed Tenable Security Center instances that are running a different version of Tenable Security Center.

If you have already installed and configured the Tenable Security Center instances you plan to manage with Tenable Security Center Director, do one of the following:

- Download and install the same version of Tenable Security Center Director that you are already running on your Tenable Security Center instances.
- Plan to upgrade your managed Tenable Security Center instances to the same version as your Tenable Security Center Director.

For more information about managing Tenable Security Center instances with Tenable Security Center Director, see Tenable Security Center Director Deployments.

Disable Default Web Servers

Tenable Security Center 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 Security Center Director to use a different port after installation.

To identify which services are listening on port 443, run the following command:

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

If there are any services listening on port 443, you must either disable them or configure them to use a different port.

Modify Security Settings

Tenable Security Center 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 installation or upgrade, the installer adds a file named `SecurityCenter` to `/etc/logrotate.d/` that contains log rotation 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 Security Center Director to communicate with Tenable servers for product and plugin updates, Tenable recommends adding Tenable sites to an allow list at your perimeter firewall.

For more information, see the knowledge base article.

Connect a PostgreSQL Server

You must configure an external PostgreSQL database if your Tenable Security Center Director installation meets any of the following criteria:

- Your Tenable Security Center Director instance has over 100,000 assets.
- Your Tenable Security Center Director instance is a non-rpm installation.

Before you install or upgrade Tenable Security Center Director, you must configure specific environment variables to connect the PostgreSQL server.

For more information, see Connect an External PostgreSQL Server.

Using the Managed PostgreSQL Server

If your deployment uses a Tenable Security Center Director managed PostgreSQL server, you can configure the `tns` account environment variables.

For information about external PostgreSQL servers, see External PostgreSQL with Tenable Security Center Director.

> **Note:** For a fresh install, you must set the environment variables with a `root` user account. If you are upgrading a previous installation with new PostgreSQL values, you must modify the values in the `/opt/sc/.pgvars` file. The values in the `.pgvars` file will be the source for connecting to the defined PostgreSQL server.

The following are the default environment variable settings:

- `SC_PG_HOST`: 127.0.0.1
- `SC_PG_USER`: tns
- `SC_PG_PORT`: 5432
- `SC_PG_PASSWORD`: {empty}
- `SC_PG_DATABASE`: SecurityCenter
- `SC_PG_CA_PATH`: {empty}
- `SC_PG_REQUIRE_TLS`: prefer

The managed PostgreSQL server can be configured to use SSL connections. Configure the following environment variables to accomplished the desired level of security:

- `SC_PG_CA_PATH` - The absolute path to the cert file. When you specify the location of the root certificate, Tenable Security Center Director verifies the root certificate used by PostgreSQL.

- `SC_PG_REQUIRE_TLS` - Whether PostgreSQL uses SSL. If this variable is not set, `ssl_mode` defaults to `prefer`. Valid values: `require`, `prefer`, `verify-ca`, `verify-full`.

Install Tenable Security Center Director

Required Tenable Security Center User Role: Root user

Tenable Security Center Director is a Linux-only application, and this topic assumes a basic understanding of Linux. To deploy Tenable Security Center as a preconfigured virtual appliance in a Windows-centric virtual environment, see the Tenable Core documentation.

For information about new features, resolved issues, third-party product updates, and supported upgrade paths, see the release notes for Tenable Security Center Director6.10.x.

Note: If your Tenable Security Center Director will manage more than 10,000 active IPs, you must update the Apache configuration file after you install and before you use Tenable Security Center Director.

Caution: During the installation process, Tenable Security Center produces a log file and saves it in the `/opt/sc/admin/logs/` directory. Tenable Security Center names the file `sc.install.log` if the installation succeeds, or `tmp.install.log` if the installation fails. Do not remove or modify these files. They are important for debugging a failed installation.

Before you begin:

- Complete system prerequisites, as described in Before You Install.
- Connect an external PostgreSQL database if your Tenable Security Center Director installation meets any of the following criteria:
  - Your Tenable Security Center Director instance has over 100,000 assets.
  - Your Tenable Security Center Director instance is a non-rpm installation.
- Download the installation RPM file from the Tenable Security Center 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 Security Center downloads page, as described in the knowledge base article.
- If your organization requires Tenable Security Center 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 Security Center Director:

1. On the host where you want to install Tenable Security Center Director, open the command line interface (CLI).
2. In the CLI, run one of the following commands to install the RPM:

   Caution: When you perform a `sudo` install, use `sudo -i` to ensure the proper use of environmental variables.

   Run the following command to install the RPM, where the file name is the RPM that you downloaded from the Tenable Security Center downloads page:

   ```
   # dnf install SecurityCenter-x.x.x-el9.x86_64.rpm
   ```

   Output similar to the following appears:

   ```
   # dnf install SecurityCenter-6.x.x-el9.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  ]
#
```

Tenable Security Center Director installs the package into `/opt/sc` and attempts to start all required daemons and web server services.

Caution: During the installation process, Tenable Security Center produces a log file and saves it in the `/opt/sc/admin/logs/` directory. Tenable Security Center names the file `sc.install.log` if the installation succeeds, or `tmp.install.log` if the installation fails. Do not remove or modify these files. They are important for debugging a failed installation.

Tip: In rare cases, you must restart the system after installation to start all services. For more information, see Start, Stop, or Restart Tenable Security Center Director.

What to do next:

- If you manage more than 10,000 active IPs, update the Apache configuration file before you use Tenable Security Center Director.

Quick Setup

The Tenable Security Center Director Quick Setup Guide walks through the following configurations:

After configuring, Review and confirm.

License

Note: These settings are not available in Tenable Enclave Security.

Caution: Do not open the license key file in a text editor. Opening the file in a text editor can corrupt it and prevent Tenable Security Center from accepting the license.

Upload your Tenable Security Center Director license.

Tenable Security Center Director License

1. Click **Choose File** to upload the Tenable Security Center Director license file you received from Tenable.

   The file should follow the format:

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

2. Click **Activate**.

   The page confirms successful upload and activation of a valid license.

Activation Codes

Consider adding additional license activation codes to allow Tenable Security Center Director to update plugins:

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

  In the **Tenable Nessus** section, type the Tenable Security Center activation code and click **Register**.

- Tenable Network Monitor license activation code – required before using and managing attached Tenable Network Monitor scanners.

  In the **Tenable Network Monitor** section, type the Tenable Network Monitor 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 Security Center initiated a plugin download in the background.

The download may take several minutes and must complete before initiating any Tenable Nessus scans. After the download completes, the **Last Updated** date and time update on the Plugins page.

Connect Tenable Security Center Instances

> **Note:** These settings are not available in Tenable Enclave Security.

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

Organization

> **Note:** These settings are not available in Tenable Enclave Security.

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

> **Note:** These settings are not available in Tenable Enclave Security.

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 Security Center. 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 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.

Check System Requirements

Before you begin the upgrade, verify that the target system still meets the hardware and software requirements for your specific deployment size. New versions of Tenable Security Center Director may introduce updated resource requirements or supported operating system versions.

> **Note:** Recommended hardware specifications were updated as of version 6.7.0. While the upgrade process does not block systems that fall below these specifications, you may experience performance degradation. Tenable Support may require hardware upgrades to resolve certain support cases.

For more information, see System Requirements.

Tenable Security Center Director Upgrade Path

Verify that your current version of Tenable Security Center Director can upgrade directly to the latest version. Some versions require a multi-step upgrade process.

For more information about supported upgrade paths, see the Tenable Security Center Release Notes.

Verify Your Plugin Set is Up to Date

If your plugin set is more than 30 days old, the upgrade will fail. Ensure you have updated your plugin set within the last 30 days before you upgrade Tenable Security Center Director. For instructions on how to update your plugins, see Edit Plugin and Feed Settings and Schedules.

Note: If the upgrade fails with an error indicating that your plugins are too old, update your plugins and then retry the upgrade. To update your plugins, log in to Tenable Security Center Director and navigate to **System** > **Configuration** > **Plugins/Feed**. For more information, see Edit Plugin and Feed Settings and Schedules.

Plan Your Tenable Security Center Director Deployment Upgrade

You must run the same version of Tenable Security Center on your entire Tenable Security Center Director deployment, including Tenable Security Center Director and all managed Tenable Security Center instances that you connect to Tenable Security Center Director. Tenable Security Center Director cannot communicate with managed Tenable Security Center instances that are running a different version of Tenable Security Center.

If you upgrade Tenable Security Center Director, you must also upgrade your managed Tenable Security Center instances to the same version to avoid communication disruptions between Tenable Security Center Director and your managed Tenable Security Center instances.

For more information about managing Tenable Security Center instances with Tenable Security Center Director, see Tenable Security Center Director Deployments.

Java Version Requirements

Tenable Security Center Director reporting requires Oracle Java JRE or OpenJDK. If you do not have Java installed, Tenable Security Center 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 ensure Tenable Security Center reporting functions correctly.

Halt or Complete Running Jobs

Tenable recommends stopping all running Tenable Security Center Director processes before beginning an upgrade. If processes are running (for example, Tenable Nessus scans), Tenable Security Center displays the following message along with the active 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 wait for the jobs to complete before retrying the upgrade.

To stop processes running on Tenable Security Center Director:

1. Log in to Tenable Security Center Director via the command line interface (CLI).
2. Stop Tenable Security Center Director with the following command:

   ```
   # /bin/systemctl stop SecurityCenter
   ```

   Tenable Security Center Director stops.
3. In the CLI in Tenable Security Center Director, 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
   ```
5. If necessary, repeat step 4 to confirm all processes stopped.

Perform a Tenable Security Center Director Backup

Tenable highly recommends performing a full backup of Tenable Security Center Director before beginning an upgrade to prevent data loss in the event of an upgrade failure.

For more information, see Backup and Restore.

Rename Your Mount Point

If your `/opt/sc` directory is a mount point or contains a mount point to another location, rename the mount point before upgrading. If the RPM upgrade process discovers a mount point, a message appears with further instructions. Contact your system administrator for assistance.

Verify Your PostgreSQL Server

Ensure your PostgreSQL server is functional before starting the upgrade. The upgrade will fail if the configured PostgreSQL server (internal or external) is unreachable or non-functional.

Note: If you are transitioning from a managed (internal) PostgreSQL server to an external PostgreSQL server, Tenable recommends performing the transition either before or after the upgrade, not during the upgrade process.

Upgrade Tenable Security Center Director

Required Tenable Security Center User Role: Root user

Note: This topic assumes a basic understanding of Linux.

Caution: During the upgrade process, Tenable Security Center produces a log file and saves it in the `/opt/sc/admin/logs/` directory. Tenable Security Center names the file `sc.install.log` if the upgrade succeeds, or `tmp.install.log` if the upgrade fails. Do not remove or modify these files. They are important for debugging a failed upgrade.

Caution: If your plugin set is more than 30 days old, the upgrade will fail. Ensure you have updated your plugin set within the last 30 days before you upgrade Tenable Security Center Director. For instructions on how to update your plugins, see Edit Plugin and Feed Settings and Schedules.

For information about new features, resolved issues, third-party product updates, and supported upgrade paths, see the release notes for Tenable Security Center Director 6.10.x.

These steps describe how to upgrade to the latest version of Tenable Security Center Director from a previous version. You can also use these steps to upgrade from an early access version of Tenable Security Center Director.

> **Note:** If you are upgrading from Tenable Security Center Director version 6.2.1 or earlier to version 6.3.x or later, you must update the Apache configuration file after you upgrade and before you use Tenable Security Center Director.

Before you begin:

1. Complete system prerequisites, as described in Before You Upgrade.

   > **Note:** Tenable recommends creating a backup of your Tenable Security Center Director data before upgrading, as described in Perform a Backup.

2. 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.
3. Confirm the integrity of the upgrade RPM file by comparing the download checksum with the checksum on the Tenable downloads page.
4. If your organization requires Tenable Security Center 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 Security Center Director 6.10.x:

1. Log in to Tenable Security Center Director via the user interface.
2. Prepare the upgrade command you intend to run:
   - Use `dnf` with the `upgrade` switch from the command line of the Tenable Security Center Director server.

- Use "`sudo -i`" when performing `sudo` upgrades of Tenable Security Center Director to ensure the proper use of environmental variables.

  > **Note:** If you are using `sudo` to perform the upgrade with a non-root user account, you must specify the full absolute path to the RPM file, even if you are executing the command from within the directory containing the file.

For example:

```
# dnf upgrade SecurityCenter-x.x.x-el9.x86_64.rpm
```

The upgrade begins. Tenable Security Center Director is not available until the upgrade finishes.

```
# dnf upgrade SecurityCenter-x.x.x-el9.x86_64.rpm
Preparing...                ########################################### [100%]
Shutting down SecurityCenter services: [  OK  ]
Backing up previous application files ... complete.
   1:SecurityCenter         ########################################### [100%]

Applying database updates ... complete.
Beginning data migration.
Starting plugins database migration...complete.
(1 of 4) Converting Repository 1 ...  complete.
(2 of 4) Converting Repository 2 ...  complete.
(3 of 4) Converting Repository 3 ...  complete.
(4 of 4) Converting Repository 4 ...  complete.
Migration complete.
Starting SecurityCenter services: [  OK  ]
~]#
```

What to do next:

- If you are upgrading from Tenable Security Center Director version 6.2.1 or earlier to Tenable Security Center Director version 6.3.x or later, update the Apache configuration file before

using Tenable Security Center Director.

- (Optional) If you used custom Apache SSL certificates before upgrading Tenable Security Center Director, restore the custom SSL certificates, as described in Restore Custom SSL Certificates.
- If you are connecting existing Tenable Security Center instances to Tenable Security Center Director for the first time, confirm that each managed instance has the required Managed Tenable Security Center license before connecting it. For more information, see Connect a Managed Tenable Security Center Instance.

Restore Custom SSL Certificates

Required Tenable Security Center User Role: Root user

If you used custom Apache SSL certificates before upgrading Tenable Security Center Director, you must restore the custom Apache SSL certificates after you upgrade Tenable Security Center Director.

Tenable Security Center Director creates a backup of the certificates during the upgrade process. Tenable Security Center 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 and reports it in the `/opt/sc/admin/log/install.log` file.

Before you begin:

- Upgrade to a new version of Tenable Security Center Director, as described in Upgrade Tenable Security Center Director.

To restore custom SSL certificates after upgrading Tenable Security Center Director:

1. Log in to Tenable Security Center Director via the command line interface (CLI).
2. In the CLI in Tenable Security Center Director, run the following command:

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

3. Select `yes` to overwrite the existing file.
4. In the CLI in Tenable Security Center Director, run the following command:

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

5. Select `yes` to overwrite the existing file.

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

6. 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
```

7. In the CLI in Tenable Security Center Director, run one of the following commands to restart the Apache server:

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

   -or-

```
# service SecurityCenter restart
```

   The Apache server restarts.

Update the Apache Configuration File

Required Tenable Security Center User Role: Root user

Tenable Security Center Director 6.3.x updated the Apache web server configuration to resolve a memory leak issue. When your Tenable Security Center Director instance meets the following criteria, you must update some values in the Apache configuration file located at `/opt/sc/support/conf/mpm.conf`:

- You are upgrading to Tenable Security Center Director version 6.10.x from version 6.2.1 or earlier.

  -or-

- Your Tenable Security Center Director instance manages more than 10,000 active IPs.

The default settings in the Apache configuration file are sufficient if you are upgrading from Tenable Security Center Director version 6.3.x or later, and your instance manages fewer than 10,000 active IPs.

Before you begin:

- Stop Tenable Security Center Director, as described in Start, Stop, or Restart Tenable Security Center Director.
  a. Stop Tenable Security Center with the following command:

  ```
  /scbase/SC.sh stop
  ```

  b. In the CLI in Tenable Security Center, run the following command to view all running processes:

  ```
  ps -fu tns
  ```

  c. If any processes are listed, run the following commands to stop them:

  ```
  killall -u tns
  killall httpd
  ```

> **Note:** These commands stop all jobs (including scans) running on Tenable Security Center.

d. If necessary, repeat step c to confirm all processes are stropped.

- Install Tenable Security Center Director or Upgrade Tenable Security Center Director

To update the Apache configuration file:

1. Navigate to the Apache configuration file, located at `/opt/sc/support/conf/mpm.conf`
2. Update the values in the configuration file. Tenable recommends the following settings based on the size of your deployment:

# Hosts Managed by Tenable Security Center Director	Recommended Settings

Fewer than 10,000 active IPs	`StartServers 5`
	`MinSpareServers 5`
	`MaxSpareServers 10`
	`MaxRequestWorkers 32`

10,000 to 25,000 active IPs	`StartServers 10`
	`MinSpareServers 10`
	`MaxSpareServers 20`
	`MaxRequestWorkers 64`

25,001 to 100,000 active IPs	`StartServers 20`
	`MinSpareServers 20`
	`MaxSpareServers 40`
	`MaxRequestWorkers 128`

# Hosts Managed by Tenable Security Center Director	Recommended Settings

100,001 or more active IPs	`StartServers 40`
	`MinSpareServers 40`
	`MaxSpareServers 80`
	`MaxRequestWorkers 256`

3. Restart Tenable Security Center Director, as described in Start, Stop, or Restart Tenable Security Center Director.

What to do next:

- After the Tenable Security Center Director build has run for a period of time, check the log located at `/opt/sc/support/logs/error_log` for any errors related to the **MaxRequestWorkers** setting. For more information, see Generate a Diagnostics File.

Uninstall Tenable Security Center Director

> **Required Tenable Security Center User Role:** Root user

This topic describes how to remove Tenable Security Center Director from your Linux host.

When you uninstall Tenable Security Center Director, the software is removed from the system, but some configuration and user data may remain in the installation directory. To completely remove all Tenable Security Center Director data, you must manually delete the installation directory.

Before you begin:

- If you want to migrate your data or keep a record of your configurations, perform a backup before uninstalling Tenable Security Center Director.

To uninstall Tenable Security Center Director:

1. Log in to the host where Tenable Security Center Director is installed.
2. Open the command line interface (CLI).
3. Stop the Tenable Security Center Director service by running the following command:

   ```
   # /bin/systemctl stop SecurityCenter
   ```

4. Remove the Tenable Security Center Director package by running the following command:

   ```
   # dnf remove SecurityCenter
   ```

5. (Optional) To remove all remaining user-created and user-modified files, run the following command:

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

   Tenable Security Center Director is removed.

What to do next:

- Ensure no Tenable processes (for example, `httpd` or `tns`) are still running by using the `ps -fu tns` command.
- Review your perimeter and host-based firewalls to remove any rules specifically created for Tenable Security Center Director (for example, port 443 access).
- If you used an external PostgreSQL server, uninstalling Tenable Security Center Director does not remove your data from the external server. You must manage that data separately on the PostgreSQL host.

User Access

The **Users** page provides the ability to add, edit, delete, or view the details of Tenable Security Center 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 Security Center Director supports three types of user account authentication: TNS, LDAP, and SAML. For more information, see User Accounts.

To log in to the Tenable Security Center 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 Tenable Security Center User Role: Any

To log in to the Tenable Security Center 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 Security Center Director web interface using a secure web connection (HTTPS) with SSL/TLS 1.2 enabled. Tenable Security Center 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 Security Center Director: *https://<SERVER ADDRESS OR NAME>/*.

Where *<SERVER ADDRESS OR NAME>* is the IPv4 or IPv6 address or hostname for your Tenable Security Center Director.

The Tenable Security Center 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 Security Center Director, see Initial Login Considerations.

   - To log in via a username and password, type your Tenable Security Center 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 Security Center 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 Security Center Director for the first time, Tenable Security Center 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 Security Center Director, see Get Started With Tenable Security Center Director.

Log in to the Web Interface via SSL Client Certificate

Required Tenable Security Center User Role: Any

Before you begin:

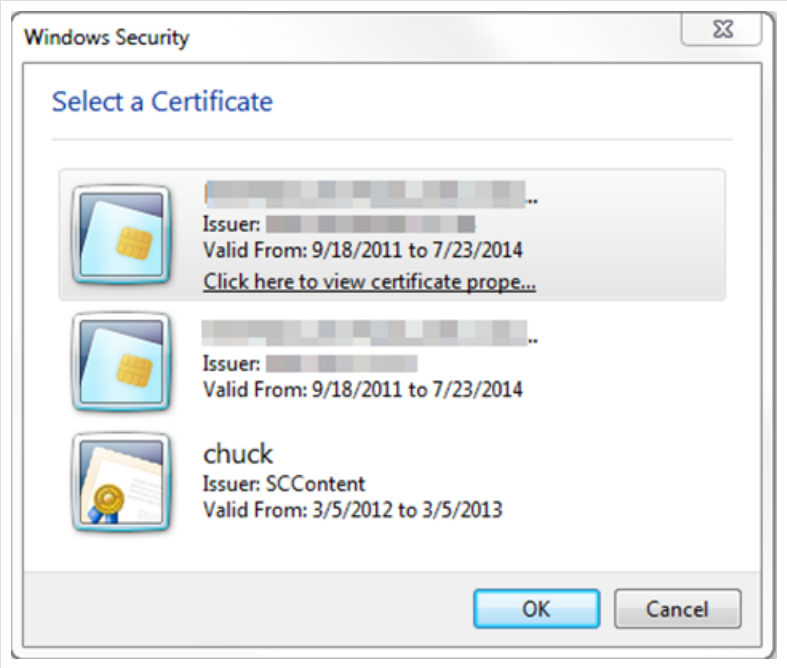
- Confirm your Tenable Security Center Director administrator fully configured Tenable Security Center Director for certificate authentication, as described in SSL Client Certificate Authentication.

To perform a certificate-based Tenable Security Center 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 Security Center Director.

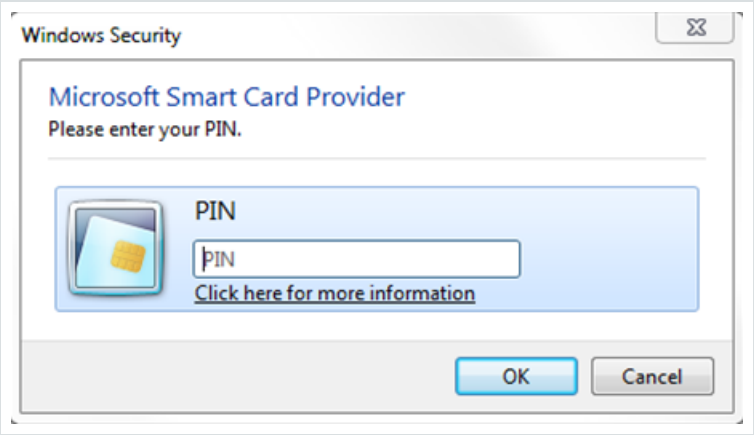
   The browser presents a list of available certificate identities.



   For information about Tenable Security Center 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 Security Center Director login page appears.
6. Log in using the username to be associated with the selected certificate.

   Caution: Only one Tenable Security Center 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 Security Center logs you in.

Subsequent Logins

After you log out of Tenable Security Center Director, the login page appears. 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

To access the **Roles** page, click **Users** > **Roles**.

Roles determine what a user can or cannot access from their account. Tenable Security Center 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.

You can create *linked user accounts* and *linked non-admin user accounts* to allow users to switch between accounts without logging out and logging back in to Tenable Security Center Director. For more information, see Linked User Accounts.

For more information about user roles in Tenable Security Center Director, see Manage User Roles.

Roles

User Role	Customizable Permissions?	Description
Administrator	No	An account that manages Tenable Security Center Director as a whole. The primary task of the Administrator is to install and configure each organization and connect managed Tenable Security Center 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 Security Center Director.
Organizational User Roles		
Security Manager	No	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 can 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 the user can launch scans, configure users (except for the Administrator user), vulnerability policies, and other objects that belong to their organization. This initial Security Manager account cannot be deleted without deleting the entire organization. Security Managers have complete access to all data collected by their organization.
SM-Linked	No	A linked account that has the same abilities as a Security Manager, except an SM-Linked account cannot configure users.
Auditor	Yes	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 create tickets.
Credential Manager	Yes	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.
Executive	Yes	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.
Security Analyst	Yes	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 freeze windows or updating plugins.
Vulnerability Analyst	Yes	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.
No Role	No	An account with virtually no permissions. No Role is assigned to a user if their designated role is deleted.
Custom Role	Yes	A custom role that you create by enabling or disabling individual permissions.

Role Options

Permissions Option	Description
General	
Name	Custom role name
Description	Custom role description
Scanning Permissions	
Create Scans	Allows the user to create policy-based scans. Disabling **Create Policies** while enabling this permission allows you to lock user into specific set of policies for scanning.
Create Plugin Scans	(Appears when **Create Scans** is enabled) Allows the user to create single plugin remediation scans.
Create Agent Synchronization Jobs	Allows the user to add agent synchronization jobs that fetch agent scan results from Tenable One Vulnerability Management or Tenable Nessus Manager.
Create Agent Scans	Allows the user to add agent scans that create and launch parallel scans in Tenable Nessus Manager, then import the scan results to Tenable Security Center.
Create Audit Files	Allows the user to upload audit files, which can be used for configuration audit scans.
Create Policies	Allows the user to set scan parameters and select plugins for scanning.
Upload Nessus Scan Results	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.

Permissions Option	Description
Manage Freeze Windows	Allows the user to add, edit, and delete organization-wide freeze windows. Freeze windows prevent scans from launching and stop any scans in progress.
Asset Permissions	
Create LDAP Query Assets	Allows the user to create LDAP Query Assets, which update a list of hosts based on a user-defined LDAP query.
Analysis Permissions	
Accept Risks	Allows the user to accept risks for vulnerabilities, which removes them from the default view for analysis, dashboards, and reports.
Recast Risks	Allows the user to change the severity for vulnerabilities.
Manage Risks	(Appears when **Accept Risks** or **Recast Risks** is enabled) Allows the user to modify accept and recast risk rules created by other users.
Organizational Permissions	
Share Objects Between Groups	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 can use the objects for filtering and scan creation.
View Organization Logs	Allows the user to view logs for entire organization.
User Permissions	
Manage Roles	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.

Permissions Option	Description
Manage Groups	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.
Manage Group Relationships	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.
Report Permissions	
Manage Images	Allows the user to upload images, so anyone in the organization can use the images in reports.
Manage Attribute Sets	Allows the user to add, edit, and delete attribute sets.
System Permissions	
Update Feeds	Allows the user to request a plugin update or a Tenable Security Center feed update.
Workflow Permissions	
Create Alerts	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.
Create Tickets	Allows the user to create tickets, which are typically used to delegate work to other users.
Asset Criticality Rating Permissions	
Manage Asset	Allows the user to manage Asset Criticality Rating scores for Asset

Permissions Option	Description
Criticality Rating	Hosts.
Host Assets Permissions	
View Host Assets	Allows the user to view the **Host Assets** page. **Note:** This permission does not restrict which host assets a user can view. The **Host Assets** page only displays hosts in the user's assigned repositories.

Manage User Roles

Required Tenable Security Center 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.

Create a User Role

To create a custom user role:

1. Log in to Tenable Security Center 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**.

   The **Add Role** page appears.
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 following permissions, as described in User Roles:
    - **Scanning Permissions**
    - **Asset Permissions**
    - **Analysis Permissions**
    - **Domain Permissions**
    - **Organization Permissions**
    - **User Permissions**
    - **Reporting Permissions**
    - **System Permissions**
    - **Workflow Permissions**
7. Click **Submit**.

    Tenable Security Center Director saves your configuration.

View User Role Details

To view role details:

1. Log in to Tenable Security Center 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. Right-click the row for the user role you want to view.

    The actions menu appears.

    -or-

    Select the check box for the user role you want to view.

    The available actions appear at the top of the table.

4. Click **View**.

   The **View Role** page appears.

Section	Action
General	View general information for the user role. • **Name** – The user role name. • **Description** – The user role description. • **User Count** – The number of users with this role. • **Created** – The date the user role was created. • **Last Modified** – The date the user role was last modified. • **ID** – The user role ID.
Scanning Permissions	View a summary of permissions for the role. For more information, see User Roles.
Asset Permissions	
Analysis Permissions	
Organization Permissions	
User Permissions	
Reporting Permissions	
System Permissions	

Section	Action
Workflow Permissions	

Edit a User Role

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

1. Log in to Tenable Security Center 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. Right-click the row for the user role you want to edit.

   The actions menu appears.

   -or-

   Select the check box for the user role you want to edit.

   The available actions appear at the top of the table.
4. Click **More** > **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**
   - **Domain Permissions**

- **Organization Permissions**
- **User Permissions**
- **Reporting Permissions**
- **System Permissions**
- **Workflow Permissions**

8. Click **Submit**.

   Tenable Security Center Director saves your configuration.

Delete a User Role

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

To delete a custom or system-provided user role:

1. Log in to Tenable Security Center 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. Select the role you want to delete:
   - To delete a single user role:
     a. In the table, right-click the row for the role you want to delete.

        The actions menu appears.

     b. Click **Delete**.
   - To delete multiple user roles:
     a. In the table, select the check box for each role you want to delete.

        The available actions appear at the top of the table.

     b. At the top of the table, click **More** > **Delete**.

A confirmation window appears.

4. Click **Delete**.

   Tenable Security Center 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 Security Center Director. *Groups* refers to collections of users with the same permissions within an organization.

Organizations

An *organization* is a set of distinct users and groups and the resources (for example, 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 Security Center Director prompts you to create the initial security manager user.

For more details, see Manage Organizations.

To view the users in an organization, filter by the organization on the Users page. For more information about filters, see Apply a Filter.

Organization Settings

Option	Description
General	
Name	(Required) The organization name.
Description	A description for the organization.
Contact Information	The relevant contact information for the organization including address, city, state, country, and phone number.
Password Expiration	
Enable Password Expiration	When enabled, passwords for users in the organization will expire after the number of days specified in the **Expiration Days** box.
Expiration Days	The number of days before the user's password expires. You can enter a number between 1 and 365. The user will receive daily password expiration notifications at login, starting 14 days before the password expires. After the password expires, the user must change their password at the next login. For more information about Tenable Security Center notifications, see Notifications.
Scanning	
Distribution Method	The scan distribution mode you want to use for this organization: • **Automatic Distribution Only**: Tenable Security Center

Option	Description
	chooses one or more scan zones to run the scan. Organizational users cannot choose a scan zone when configuring a scan. Tenable Security Center distributes targets for scans based on your configured scan zone ranges. This facilitates optimal scanning and is useful if an organization has devices placed behind a firewall or NAT device or has conflicting RFC 1918 non-internet-routable address spaces. • **Locked Zone**: Tenable Security Center uses the one **Available Zone** you specify to run the scan. Organizational users cannot modify the scan zone when configuring a scan. • **Selectable Zones**: Tenable Security Center allows organizational users to select a scan zone when configuring a scan. 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. • **Linked**: Tenable Security Center runs the organization's scans through linked Tenable Nessus scanners, which connect to Tenable Security Center through a Sensor Proxy. When you select **Linked**, the **Prefer Linked Scan Zones** setting appears. For more information about linked scanning, see Linked Scanning Overview. For more information about scan zones, see Scan Zones.
Available Zones	One or more scan zones that you want organizational users to have

Option	Description
	access to when configuring scans.
Allow for Automatic Distribution	Enable or disable this option to specify whether you want Tenable Security Center to select one or more scan zones automatically if an organizational user does not specify a scan zone when configuring a scan. • When enabled, Tenable Security Center chooses one or more scan zones as specified by your **Restrict to Selected Zones** setting. • When disabled, Tenable Security Center requires the organizational user to specify a scan zone when configuring a scan.
Restrict to Selected Zones	If **Allow for Automatic Distribution** is enabled, enable or disable this option to specify the zones you want Tenable Security Center to choose from when automatically distributing zones. • When enabled, Tenable Security Center chooses from the **Available Zones** shared with the organization. • When disabled, Tenable Security Center chooses from all zones on Tenable Security Center.
Restricted Scan Ranges	The IP address ranges you do not want users in this organization to scan.
Prefer Linked Scan Zones	Appears when **Distribution Method** is set to **Linked**. Determines whether Tenable Security Center Director prefers linked Tenable Nessus scanners or active (managed) Tenable Nessus scanners when a scan's targets fall within scan zones that contain both types and either could perform the scan.

Option	Description
	When enabled, Tenable Security Center Director tries a linked scanner first. If no linked scanner in an eligible zone can cover the scan, Tenable Security Center Director uses an active scanner. When disabled (default), Tenable Security Center Director tries an active scanner first. If no active scanner in an eligible zone can cover the scan, Tenable Security Center Director uses a linked scanner. If only one type of scanner can cover the scan, Tenable Security Center Director uses that type regardless of this setting. If no scanner of either type can cover all of the scan's targets, the scan fails. **Note:** Linked scans always enforce scan zone IP ranges. Scans whose targets include asset lists or asset tags are not eligible for linked scanning in this release and run as active scans. For more information, see Linked Scanning Overview.
Analysis	
Accessible Repositories	The repositories that you want this organization to have access to. You can search for the repositories by name or scroll through the list.
Accessible Agent Capable Scanners	The Tenable Nessus scanners (with Tenable 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 Tenable Agent results from the selected scanner.
Accessible LDAP Servers	The LDAP servers that you want this organization to have access to. An organization must have access to an LDAP server to perform LDAP authentication on user accounts within that organization, and to configure LDAP query assets.

Option	Description
	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 Security Center 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 Security Center. 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	
Low	The vulnerability weighting to apply to **Low** criticality vulnerabilities for scoring purposes. (Default: 1)
Medium	The vulnerability weighting to apply to **Medium** criticality vulnerabilities for scoring purposes. (Default: 3)
High	The vulnerability weighting to apply to **High** criticality vulnerabilities for scoring purposes. (Default: 10)
Critical	The vulnerability weighting to apply to **Critical** criticality vulnerabilities for scoring purposes. (Default: 40)
Vulnerability Scoring System	
Scoring System	The scoring system Tenable Security Center Director uses to assess the severity of vulnerabilities: **CVSS v2**, **CVSS v3**, or **CVSS v4**.

Option	Description
	Note: Changing the **Scoring System** while Tenable Security Center Director is running certain operations, such as preparing reports or dashboard data, results in data using mixed CVSS v2, CVSS v3, and CVSS v4 scores. **Note:** Changing the **Scoring System** does not impact historical dashboard trend data. For example, if you change the **Scoring System** from **CVSS v3** to **CVSS v4**, dashboard trend data before the change displays CVSS v3 scores while dashboard trend data after the change displays CVSS v4 scores.
BOD 26-04 SLA	
Enabled	When selected, enables CISA BOD 26-04 for the organization. When enabled, the **BOD 26-04 Internet Facing**, **CISA SLA**, and **SLA Time Left** filters, the **CISA SLA** and **SLA Time Left** columns, and the **BOD 26-04** section of the vulnerability details appear for users in the organization. For more information, see Vulnerability Analysis Filter Components and Manage Vulnerabilities. BOD 26-04 is not enabled for an organization until you select this option. No additional license is required.
Public-Facing Asset Tag	One or more asset tags that identify public-facing assets. Tenable Security Center treats an asset as public-facing only if it has a selected tag. Assets without a selected tag have *unknown* exposure, and vulnerabilities on those assets match neither **Yes** nor **No** in the **BOD 26-04 Internet Facing** filter. When you change the selected tags, Tenable Security Center re-tiers existing findings. This may take a few minutes.

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.

For more information, see Manage Groups.

Group Settings

Option	Description
General tab	
Name	The name for the group.
Description	A description for the group (e.g., **security team at the central office** or **executives on the east coast**).
Viewable Hosts	The hosts that are viewable by users in the group. You can set this to **All Defined Ranges**, which includes all IP ranges and agent UUIDs defined across the organization's repositories, or select one or more specific asset lists to restrict access to a subset of hosts.
Repositories	The repositories you want to share with the group.
Sample Content	When enabled, Tenable provides sample content objects to users in the group: • sample dashboards (**Executive 7 Day**, **Executive Summary**, and **Vulnerability Overview**) • sample reports (**Critical and Exploitable Vulnerabilities**, **Monthly Executive**, and **Remediation Instructions by Host**)

Option	Description
	• sample ARCs (**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**) • sample assets required for the sample ARCs After enabling **Sample Content**, you must add a new user to the group before all users in the group can access the sample content. **Note:** If a user in a group deletes a sample content object, the object is deleted for all other users in that group. **Note:** If you move a sample content object owner (e.g., move the first user in group A to group B), Tenable Security Center: 1. Assigns their dashboards and ARCs to a new sample content object owner in group A. Tenable Security Center does not reassign reports or assets. 2. Recreates their dashboards, ARCs, and assets required for ARCs in group B. Tenable Security Center does not recreate reports.
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.

Manage Organizations

Required Tenable Security Center User Role: Administrator

For more information about organization options, see Organizations.

Add an Organization

To add an organization:

1. Log in to Tenable Security Center Director 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**
   - **Password Expiration**
   - **Scanning**
   - **Analysis**
   - **Custom Analysis Links**
   - **Vulnerability Weights**
   - **Vulnerability Scoring System**
   - **BOD 26-04 SLA**
5. Click **Submit**.

   Tenable Security Center Director saves your configuration.

Edit an Organization

You can edit the settings for an existing organization, including enabling CISA BOD 26-04 for the organization.

To edit an organization:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **System** > **Organizations**.

   The **Organizations** page appears.

3. Right-click the row for the organization you want to edit.

   The actions menu appears.

   -or-

   Select the check box for the organization you want to edit.

   The available actions appear at the top of the table.

4. Click **Edit**.

   The **Edit Organization** page appears.

5. Modify the organization settings. For more information about a setting, see Organization Settings.

6. To enable CISA BOD 26-04 for the organization, in the **BOD 26-04 SLA** section at the bottom of the page:

   a. Select the **Enabled** check box.

   b. In the **Public-Facing Asset Tag** box, select one or more asset tags. Tenable Security Center treats assets that have a selected tag as public-facing. For more information, see BOD 26-04 SLA.

7. Click **Submit**.

   Tenable Security Center saves your configuration. If you changed the **Public-Facing Asset Tag** selection, Tenable Security Center re-tiers existing findings. This may take a few minutes.

Note: CISA BOD 26-04 does not require an additional license. The BOD 26-04 filters, columns, and vulnerability detail section appear only for organizations where you enable it. If you do not select a public-facing asset tag, all assets have unknown exposure and match neither **Yes** nor **No** in the **BOD 26-04 Internet Facing** filter.

View Organization Details

To view organization details:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **System** > **Organizations**.

The **Organizations** page appears.

3. Right-click the row for the organization you want to view.

   The actions menu appears.

   -or-

   Select the check box for the organization you want to view.

   The available actions appear at the top of the table.

4. Click **View**.

   The **View Organization** page appears.

Section	Action
General	View general information for the organization. • **Name** – The organization name. • **Description** – The organization description. • **Address** / **City** / **State** / **Country** / **Phone** – The contact information for the organization. • **Created** – The date the organization was created. • **Last Modified** – The date the organization was last modified. • **ID** – The organization ID.
Password Expiration	View a summary of your password expiration settings for the organization. For more information about a setting, see Organizations.
Scanning	View a summary of your scanning settings for the organization. For more information about a setting, see Organizations.
Analysis	View a summary of your analysis settings for the organization. For more information about a setting, see Organizations.

Section	Action
Custom Analysis Links	View a summary of your custom analysis link settings for the organization. For more information about a setting, see Organizations.
Vulnerability Weights	View a summary of your vulnerability weights settings for the organization. For more information about a setting, see Organizations.
Vulnerability Scoring System	View the vulnerability scoring system selected for the organization. For more information, see Organizations.

Delete an Organization

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

To delete an organization:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **System** > **Organizations**.

   The **Organizations** page appears.
3. Select the organization you want to delete:
   - To delete a single organization:
     a. In the table, right-click the row for the organization you want to delete.

        The actions menu appears.

     b. Click **Delete**.
   - To delete multiple organizations:
     a. In the table, select the check box for each organization you want to delete.

        The available actions appear at the top of the table.

     b. At the top of the table, click **Delete**.

   A confirmation window appears.

4. Click **Delete**.

   A confirmation window appears.

5. Click **Delete**.

   Tenable Security Center Director deletes the organization.

Manage Groups

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

For more information about group options, see Groups.

Add a Group

To add a group:

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, click **Users** > **Groups**.

   The **Groups** page appears.

3. Click **Add**.

   The **Add Group** page appears.

4. Configure the **General** options.
5. Configure the **Share to Group** options.
6. Click **Submit**.

   Tenable Security Center Director saves your configuration.

View Group Details

To view group details:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Users** > **Groups**.

The **Groups** page appears.

3. Right-click the row for the group you want to view.

   The actions menu appears.

   -or-

   Select the check box for the group you want to view.

   The available actions appear at the top of the table.

4. Click **View**.

   The **View Group** page appears.

Section	Action
General	View general information for the group. • **Name** – The group name. • **Description** – The group description. • **Created** – The date the group was created. • **Last Modified** – The date the group options were last modified. • **ID** – The group ID.
Access	View the lists of **Viewable Hosts** and **Repositories** users in the group can access. For more information, see Group Settings.
Preferences	View whether you enabled **Sample Content** for the group. For more information, see Group Settings.
Users	View the list of users associated with the group.

Delete a Group

To delete a group:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Users** > **Groups**.

   The **Groups** page appears.
3. Select the group you want to delete:
   - To delete a single group:
     a. In the table, right-click the row for the group you want to delete.

        The actions menu appears.

     b. Click **Delete**.
   - To delete multiple groups:
     a. In the table, select the check box for each group you want to delete.

        The available actions appear at the top of the table.

     b. At the top of the table, click **Delete**.

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

   Tenable Security Center Director deletes the group.

User Accounts

The **Users** page displays the user accounts on Tenable Security Center 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 User Account or Delete a User Account.

You can create one or more administrator accounts on Tenable Security Center Director. You can create one or more organizational users (security managers and custom roles) per organization. Tenable recommends you make at least one TNS-authenticated administrator and security manager user per organization so that you can still log in if the LDAP or SAML service becomes unavailable. For more information about user account types, see User Access.

For more information about options available when configuring user accounts, see User Account Options.

Linked User Accounts

You can create *linked user accounts* and *linked non-admin user accounts* to allow users to switch between accounts without logging out and logging back in to Tenable Security Center Director. For more information, see Linked User Accounts.

API Keys

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

Add a User Account

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

You can add a TNS, LDAP, or SAML authenticated user account.

Add a TNS-Authenticated User

For more information about user account configuration options, see TNS User Account Options.

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

1. Log in to Tenable Security Center Director 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) Enable **Password Expiration** for the user.
14. (Optional) Enable **Dark Mode** for the user.
15. (Optional) Type **Contact Information** for the user.
16. Click **Submit**.

    Tenable Security Center Director saves your configuration.

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

1. Log in to Tenable Security Center Director 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. (Optional) Enable **Password Expiration** for the user.

12. Select a **Role**. For more information, see User Roles.
13. Select a **Group**. For more information, see Organizations and Groups.
14. (Optional) If you want to customize the group-related permissions for the user, modify the **Group Permissions** as described in Custom Group Permissions.
15. (Optional) If you want to share an asset list with the user, select an **Asset**. For more information, see Asset Tags.
16. (Optional) Enable **Dark Mode** for the user.
17. (Optional) Type **Contact Information** for the user.
18. Click **Submit**.

    Tenable Security Center Director saves your configuration.

Add an LDAP-Authenticated User

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 Security Center Director 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 Manage LDAP Servers.
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) Enable **Dark Mode** for the user.
18. (Optional) Type **Contact Information** for the user.
19. Click **Submit.**

    Tenable Security Center Director saves your configuration.

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

1. Log in to Tenable Security Center Director 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 Manage LDAP Servers.
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 Asset Tags.
17. (Optional) Enable **Dark Mode** for the user.
18. (Optional) Type **Contact Information** for the user.
19. Click **Submit**.

    Tenable Security Center Director saves your configuration.

Add a SAML-Authenticated User

For more information about user account configuration options, see SAML User Account Options. To automatically add SAML-authenticated users by importing users from your SAML identity provider, see Configure SAML User Provisioning.

Before you begin:

- Review the Tenable SAML Configuration Quick-Reference guide for a step-by-step guide of how to configure SAML for use with Tenable Security Center Director.
- 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 Security Center Director 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) Enable **Dark Mode** for the user.
11. (Optional) Type **Contact Information** for the user.
12. Click **Submit**.

    Tenable Security Center Director saves your configuration.

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

1. Log in to Tenable Security Center Director 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 Asset Tags.

14. (Optional) Enable **Dark Mode** for the user.

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

16. Click **Submit**.

    Tenable Security Center Director saves your configuration.

Manage User Accounts

For more information about user accounts, see User Accounts.

View User Account Details

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

To view the details of any user account:

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

   The **Users** page appears.
3. Right-click the row for the user you want to view.

   The actions menu appears.

   -or-

   Select the check box for the user you want to view.

   The available actions appear at the top of the table.
4. Click **View**.

   The **View User** page appears.
5. View the following information for the user:

Section	Action
General	View general information for the user. • **Created** – The date the user was created. • **Last Modified** – The date the user was last modified. • **ID** – The user ID.
Membership	View role and organization information for the user. For more information, see User Account Options.
Password Expiration	View password expiration settings for the user. For more information, see User Account Options.

Display Options	View dark mode settings for the user. For more information, see User Account Options.
Contact Information	View contact information for the user. For more information, see User Account Options.
API Key	If the user has API keys, view the access key for the user. For more information, see Enable API Key Authentication.
Linked User Details	**Required Tenable Security Center 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. If the user is a Security Manager, view the linked SM-Linked users. • **Primary User** – If the user is a linked Security Manager, view the associated Administrator user. If the user is an SM-Linked user, view the associated Security Manager user. For more information, see Linked User Accounts.

Filter the Users Page

Required Tenable Security Center User Role: Any

To filter the user accounts on the **Users** page:

1. Log in to Tenable Security Center 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.

> **Note:** If you are logged in with an administrator account, the **Organization** filter is set to **System** by default. To view users from other organizations, select a different organization for the **Organization** filter.

Edit Your User Account (Administrator)

> **Required Tenable Security Center User Role:** Administrator

You can edit your user account to update your password, contact information, display preferences, and other settings depending on your user role. If you want to edit a linked user account, see Manage Linked Users.

> **Note:** The username can be changed for all users except the first Security Manager and the first administrator of each organization.

To edit your user account as an administrator:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **System**> **Users**.

   The **Users** page appears.
3. Right-click the row for your user account.

   The actions menu appears.

   -or-

   Select the check box for your user account.

   The available actions appear at the top of the table.
4. Click **More** > **Edit**.

   The **Edit User** page appears.
5. Modify your user account settings. For more information, see User Account Options.

   > **Note:** If you want to edit a Tenable Security Center user that was created via user provisioning and you enabled **User Data Sync**, edit the user in your SAML or LDAP identity provider. Otherwise, the Tenable Security Center user data synchronization overwrites your changes the

next time the user logs in to Tenable Security Center using your SAML or LDAP identity provider. For more information about **User Data Sync**, see SAML Authentication Options or LDAP Authentication Options.

6. Click **Submit**.

   Tenable Security Center Director saves your configuration.

Edit Your User Account (Organizational User)

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

You can edit your user account to update your password, contact information, display preferences, and other settings depending on your user role. If you want to edit a linked user account, see Manage Linked Users.

Note: The username can be changed for all users except the first Security Manager and the first administrator of each organization.

To edit your user account as an organizational user:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Username** > **Profile**.

   The **Edit User Profile** page appears.
3. Modify your user account settings. For more information, see User Account Options.

   Note: If you want to edit a Tenable Security Center user that was created via user provisioning and you enabled **User Data Sync**, edit the user in your SAML or LDAP identity provider. Otherwise, the Tenable Security Center user data synchronization overwrites your changes the next time the user logs in to Tenable Security Center using your SAML or LDAP identity provider. For more information about **User Data Sync**, see SAML Authentication Options or LDAP Authentication Options.
4. Click **Submit**.

   Tenable Security Center Director saves your configuration.

Replace First User

Required Tenable Security Center User Role: Administrator

By default, the first user is the first Security Manager user account you create during setup. You can promote a different Security Manager account to first user to replace the previous Security Manager account.

When you replace a first user with a different Security Manager account, the promoted Security Manager will absorb the contents of the previous Security Manager's account. The promoted Security Manager account will keep both its objects and the objects of the previous Security Manager account, because that data is not cleared before the migration. After the replacement, the promoted Security Manager loses any previous notifications and running jobs.

Note: When you promote a certificate-based user account to first user, the promoted user account automatically changes to password-based authentication.

Before you begin

- These steps assume you already have more than one Security Manager account. If you do not already have a second Security Manager account, create a new user account with the Security Manager role. For more information about creating user accounts, see User Accounts.

To replace the first user with a different Security Manager user account:

1. Log in to Tenable Security Center Director via the Admin user interface.
2. Click **Users** > **Users**.

   The **Users** page appears.
3. On the left side of the page, select the organization by which you want to filter the page. For instructions on how to apply a filter, see Apply a Filter.
4. Right-click the row for the current Security Manager first user.

   The actions menu appears.

   -or-

   Select the check box for the current Security Manager first user.

The available actions appear under **More** at the top of the table.

5. Click **Replace First User**.

   The **Replace First User** window appears.

6. In the **Users** drop-down, select the Security Manager that you want to promote to first user.
7. In the **New Password** box, type a new password for the user.
8. Click **Replace**.

   The Security Manager you selected in step 5 is promoted to first user.

Delete a User Account

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

Notes:

- 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.
- You cannot delete the initially created Administrator and Security role users from any of your organizations. You can replace the initial Security Manager user. For more information, see Replace First User.
- If you want to delete an Administrator or Security Manager with linked user accounts, you must delete the linked accounts associated with the Administrator or Security Manager before deleting the Administrator or Security Manager, as described in Delete a Linked User Account. For more information about linked user accounts, see Linked User Accounts.
- If you want to delete a Tenable Security Center user that was created via user provisioning, delete the user from your SAML or LDAP identity provider. If you delete a user in Tenable Security Center that was created via user provisioning without deleting the user in your SAML or LDAP identity provider, Tenable Security Center automatically re-creates the user in Tenable Security Center the next time they log in using your SAML or LDAP identity provider. For more information, see SAML User Provisioning or LDAP User Provisioning.

To delete a user:

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

   The **Users** page appears.
3. Select the user you want to delete:
   - To delete a single user:
     a. In the table, right-click the row for the user you want to delete.

        The actions menu appears.

     b. Click **Delete**.
   - To delete multiple users:
     a. In the table, select the check box for each user you want to delete.

        The available actions appear at the top of the table.

     b. At the top of the table, click **More** > **Delete**.

   A confirmation window appears.
4. (Optional) If you want to migrate the user's objects, click the toggle to migrate the user's objects to another user. Tenable Security Center supports migrating:
   - Active scans, agent scans, and scan results
   - Custom assets, credentials, audit files, and scan policies
   - Freeze 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 Security Center deletes the user's objects.

   Note: The following are considerations for migrating objects:

- You cannot migrate objects when deleting an Administrator user because all Administrator-created objects are shared across Tenable Security Center and remain accessible after user deletion.
- If you delete a linked non-admin user, the user's objects can only be migrated to the linked Security Manager account. For more information about linked user accounts, see Linked User Accounts.
- When you delete multiple users, you cannot migrate objects for the users unless you are logged in as an Administrator.

5. Click **Delete**.

   Tenable Security Center deletes the user.

Linked User Accounts

You can create *linked user accounts* and *linked non-admin user accounts* to allow users to switch between accounts without logging out and logging back in to Tenable Security Center Director.

- **Linked User Account** - A Security Manager user account that is linked to an Administrator user account.
- **Linked Non-Admin User Account** - An SM-Linked user account that is linked to a Security Manager user account.

On the **Users** page, a tooltip appears next to linked and linked non-admin users that displays the username for the associated Administrator or Security Manager account.

For more information about user accounts in Tenable Security Center Director, see User Access and User Roles.

For more information about linked user accounts, see Manage Linked Users.

Linked User

Users with linked user accounts can use a single set of login credentials to log in to Tenable Security Center 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.
- Each linked Security Manager can be associated with only one Administrator user account.
- Linked Security Managers cannot log in to Tenable Security Center Director directly. You must log in to the Administrator account associated with 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.

Linked Non-Admin User

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

> **Note:** You must have more than one organization to create a linked non-admin user. For more information about organizations, see Organizations.

The following restrictions apply to linked non-admin user accounts:

- Each Security Manager can have one linked SM-Linked user account per organization.
- Each SM-Linked user account can be associated with only one Security Manager user account.
- SM-Linked user accounts cannot create, edit, or delete user accounts in the organization.

- SM-Linked users do not have access to the **Profile** page to edit their own accounts.
- SM-Linked users cannot log in to Tenable Security Center Director directly. You must log in to the Security Manager account associated with the SM-Linked account, then switch users.
- You can only create linked non-admin user accounts for TNS user accounts. Linked non-admin user accounts are not supported for LDAP or SAML user accounts.
- You cannot convert a standalone user account to a linked non-admin user account.
- You cannot convert an SM-Linked user to a standalone user account. To unlink an SM-Linked user from a Security Manager user, delete the SM-Linked user account.
- You cannot create a standalone SM-Linked user account.

Manage Linked Users

You can create *linked user accounts* and *linked non-admin user accounts* to allow users to switch between accounts without logging out and logging back in to Tenable Security Center Director. You can add a linked Security Manager to an Administrator account, or you can add an SM-Linked user to a Security Manager account.

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

Add a Linked User

Required Tenable Security Center User Role: Administrator

To add a linked Security Manager to an Administrator, or add an SM-Linked user to a Security Manager:

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, click **System** > **Users**.

   The **Users** page appears.
3. Right-click the row for the Administrator or Security Manager to which you want to add a linked user.

The actions menu appears.

-or-

Select the check box for the Administrator or Security Manager to which you want to add a linked user.

The available actions appear at the top of the table.

4. Click **Add Linked User**.

   The **Add User** page appears. Tenable Security Center Director pre-populates the **First Name**, **Last Name**, and **Contact Information** fields with values from the Administrator or Security Manager user account.

5. Select an **Organization**. If you create a linked non-admin user, you can select more than one organization and Tenable Security Center Director will create one linked non-admin user for each organization.
6. (Optional) Modify the **First Name** and **Last Name** for the user.
7. Type a **Username** for the user. If you create a linked non-admin user, Tenable Security Center Director adds the orgID to the end of the username.
8. Select a **Time Zone**.
9. (Optional) Select a **Scan Result Default Timeframe**.
10. (Optional) Enable **Cached Fetching**.
11. (Optional) Enable or disable **Dark Mode** for the user.
12. (Optional) Modify the **Contact Information** for the user.
13. Click **Submit**.

    Tenable Security Center Director saves your configuration.

Switch to a Linked User Account

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. Linked non-admin users can switch from the linked Security Manager to an SM-Linked user, from one SM-Linked user to another, or from an SM-Linked user to the linked Security Manager.

To switch to a linked user account:

1. Log in to Tenable Security Center Director via the user interface.

   > **Note:** You must log in to the Administrator or Security Manager account associated with the linked user, then switch between linked users. Linked Security Managers and SM-Linked users cannot log in to Tenable Security Center Director directly.

2. Click your user profile SC icon > **Switch User**. This option appears only if the current logged-in user already has a linked user account.

   The **Switch To Linked Account** window appears.

3. Click the name of the linked user you want to switch to.

4. Click **Switch**.

   Tenable Security Center Director logs you in as the selected user.

   The username menu updates to show the linked user account name and associated organization.

Edit a Linked User Account (Administrator)

> **Required Tenable Security Center User Role:** Administrator

To edit a linked user account as an Administrator:

1. Log in to Tenable Security Center Director via the user interface.

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

   The **Users** page appears.

3. Filter the **Users** page to show user accounts for the linked user's organization, as described in Apply a Filter.

4. Right-click the row for the linked user account you want to edit.

   The actions menu appears.

   -or-

   Select the check box for the linked user account you want to edit.

The available actions appear at the top of the table.

5. Click **More** > **Edit**.

   The **Edit User** page appears.

6. Modify the user account settings. For more information, see User Account Options.

7. Click **Submit**.

   Tenable Security Center Director saves your configuration.

Edit a Linked User Account (Linked User)

Required Tenable Security Center User Role: Security Manager linked to an Administrator or an SM-Linked user linked to a Security Manager. For more information, see User Roles and Linked User Accounts.

To edit your linked user account as a linked user:

1. Log in to Tenable Security Center Director via the user interface.
2. Switch to a linked user account, as described in Switch to a Linked User Account.
3. Click **Username** > **Profile**.

   The **Edit User Profile** page appears.

4. Modify the user account settings. For more information, see User Account Options.
5. Click **Submit**.

   Tenable Security Center Director saves your configuration.

Delete a Linked User Account

Required Tenable Security Center User Role: Administrator

Note:

- 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.
- If you want to delete an Administrator or Security Manager with linked user accounts, you

must delete the linked accounts associated with the Administrator or Security Manager before deleting the Administrator or Security Manager.

To delete a linked user account:

1. Log in to Tenable Security Center 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. Select the linked user account you want to delete:
   - To delete a single linked user account:
     a. In the table, right-click the row for the linked user account you want to delete.

        The actions menu appears.
     b. Click **Delete**.
   - To delete multiple linked user accounts:
     a. In the table, select the check box for each linked user account you want to delete.

        The available actions appear at the top of the table.
     b. At the top of the table, 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 Security Center Director supports migrating:
   - Active scans, agent scans, and scan results
   - Custom assets, credentials, audit files, and scan policies
   - Freeze 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 Security Center 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 Security Center Director and remain accessible after user deletion.

6. Click **Delete**.

   Tenable Security Center 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.

Resources Controlled by Manage Users/User Permissions	Resources Controlled by Manage Objects/Object Permissions
• Users (edit and delete) • Groups (edit and delete)	• Reports (launch, stop, copy, delete, and sometimes edit)

Resources Controlled by Manage Users/User Permissions	Resources Controlled by Manage Objects/Object Permissions
	Note: A user can only edit reports within their assigned group, even if you grant them **Object Permissions** for another group. • Report results (publish, email, copy, and delete) • Report images (delete) • Report attributes (delete) • Scan results (stop, pause, and delete) • Assets (edit, share, and delete) • 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*.

Manage API Keys

> **Required Tenable Security Center 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 Security Center API requests. 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 Security Center deauthorizes API requests attempted with the old keys.

Generate API Keys

Administrators can generate API keys for any user account. Other roles can generate API keys for user accounts with the same role.

> **Note:** Before you generate API keys, you must enable API key authentication. If you skip this step, the **API Keys** option does not appear in the action menu. For more information, see Enable API Key Authentication.

To generate API keys:

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

The **Users** page appears.

3. Right-click the row for the user for which you want to generate an API key.

   The actions menu appears.

   -or-

   Select the check box for the user for which you want to generate an API key.

   The available actions appear at the top of the table.

4. Click **API Keys > 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 Security Center 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 Security Center API Best Practices Guide*.

Delete API Keys

After you delete a user's API keys, the deleted keys cannot be used for authentication in Tenable Security Center API requests.

To delete API keys:

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

   The **Users** page appears.

3. Right-click the row for the user for which you want to delete API keys.

The actions menu appears.

-or-

Select the check box for the user for which you want to delete API keys.

The available actions appear at the top of the table.

4. Click **API Keys** > **Delete API Key**.

   A confirmation window appears.

5. Click **Delete**.

   The system deletes the API keys.

User Account Options

You can configure the following options for Tenable Security Center Director user accounts. The available options depend on the user type, the user's role, and the role of the user adding or editing the user.

For more information about user accounts in Tenable Security Center, see User Accounts.

TNS User Account Options

To add a TNS-authenticated user, see Add a TNS-Authenticated User.

Option	Description
First Name	The user's first name.
Last Name	The user's last name.
Type	(If LDAP or SAML are configured) The type of authentication you want to perform on the user: • Tenable (**TNS**) • Lightweight Directory Access Protocol (**LDAP**)

	• Security Assertion Markup Language (**SAML**) You must configure an LDAP server or SAML authentication in order to select **LDAP** or **SAML** from the **Type** drop-down box.
Username	(Required) The username for the user account. **Note:** The username value is case-sensitive.
Password	(Required) The password for the user account. The password must meet the minimum length and complexity requirements configured in the Security Settings of the Configuration page. For new installations, passwords must be at least 12 characters long and contain at least one uppercase letter, one lowercase letter, one numerical character, and one special character. If you upgraded to Tenable Security Center 6.10 or later, your existing password requirements remain in effect until an administrator changes them. For more information, see Security Settings. **Tip:**Tenable recommends using passwords that meet stringent length and complexity requirements. For information about Tenable Security Center Director password data encryption, see Encryption Strength. When editing a user, type a new password to change the password for the user account.
Confirm Password	(Required) When creating a user or changing a user's password, re-type the password for the user account.
Password Change	Click **Change Password** to change the password for the user account. To change a user password: 1. Begin editing a user account, as described in Manage User Accounts.

	2. Click **Change Password**. 3. In the **Current Password** box, type your password. If you do not have a password (for example, you have a SAML-authenticated or LDAP-authenticated user account), type any string of characters in this field. 4. In the **Password** box, type a new password. 5. In the **Confirm Password** box, type the new password again. 6. Click **Submit**. Tenable Security Center Director saves your configuration.
Current Password	(If you click **Change Password**) Type your password. If you do not have a password (for example, you have a SAML-authenticated or LDAP-authenticated user account), type any string of characters in this field.
User Must Change Password	When enabled, the user must change their password upon initial login.
Account Locked	When enabled, the user cannot log in to Tenable Security Center. An administrator must unlock the user's account to allow them to log in.
Time Zone	(Required) The time zone for the user.
Scan Result Default Timeframe	The default **Completion Time** filter applied when the user accesses or refreshes the scan results page.
Cached Fetching	When enabled, Tenable Security Center Director caches plugin policy information and performs plugin policy downloads once per page load.
Password Expiration	
Password Never Expires	When enabled, the user's password will never expire. Any password expiration settings at the user or organization level will not apply to this user.

Enable Password Expiration or **Custom Password Expiration**	When enabled, the user's password will expire after the number of days specified in the **Expiration Days** box. When disabled, the user's password expiration settings will default to the organization settings. For more information about organization options, see Organizations. The user will receive daily password expiration notifications at login, starting 14 days before the password expires. After the password expires, the user must change their password at the next login. For more information about Tenable Security Center notifications, see Notifications.
Expiration Days	The number of days before the user's password expires. You can enter a number between 1 and 365.
Membership	
Role	(Required) 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: • If a user is an Auditor, they can create new Auditors or lesser roles. • If a custom user has the Create Policies privilege but not the Update Feeds privilege, that user can create users with the Create Policies privilege, but not the Update Feeds privilege.
Organization	(Required) The organization where you want to assign the user account.
Group	(Required) The group where you want to assign the user account. A user's group determines their access to Tenable Security Center Director

	resources. For more information about groups, see Groups. To grant a user limited privileges to other groups' resources, see Custom Group Permissions.
Group Permissions	
Manage All Users	When enabled, allows the user to manage users in all of the user's assigned groups. For more information, see Custom Group Permissions.
Manage All Objects	When enabled, allows the user to manage objects in all of the user's assigned groups. For more information, see Custom Group Permissions.
Responsibility	
Asset	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.
Display Options	
Dark Mode	When enabled, sets the Tenable Security Center user interface to dark mode for the user.
Use System Dark Mode Setting	When enabled, the Tenable Security Center Director user interface uses the operating system setting for light or dark mode. This setting overrides the **Dark Mode** setting. If you select the sun or moon icon in the top navigation bar, that will override the **Use System Dark Mode Setting** for the user account.
Contact Information	

Title	The contact information for the user.
Address	
City	
State	
Country	
Email	
Phone	

LDAP User Account Options

You must configure an LDAP server to add LDAP-authenticated users. For more information, see LDAP Authentication.

To add an LDAP-authenticated user, see Add an LDAP-Authenticated User.

Option	Description
First Name	The user's first name.
Last Name	The user's last name.
Type	(If LDAP or SAML are configured) The type of authentication you want to perform on the user: • Tenable (**TNS**) • Lightweight Directory Access Protocol (**LDAP**) • Security Assertion Markup Language (**SAML**) You must configure an LDAP server or SAML authentication in order to select **LDAP** or **SAML** from the **Type** drop-down box.

LDAP Server	The LDAP server you want to use to authenticate the user.
Search String	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** sAMAccountName=* mail=a* displayName=C*
LDAP Users Found	A filtered list of LDAP user accounts retrieved by the **Search String**. Your selection in this option populates the **Username** option.
Username	(Required) The username, populated by your **LDAP Users Found** selection. This username must match a user on the LDAP server in order to authenticate successfully.
Time Zone	(Required) The time zone for the user.
Scan Result Default Timeframe	The default **Completion Time** filter applied when the user accesses or refreshes the scan results page.
Cached Fetching	When enabled, Tenable Security Center Director caches plugin policy information and performs plugin policy downloads once per page load.
Membership	
Role	(Required) 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: • If a user is an Auditor, they can create new Auditors or lesser roles. • If a custom user has the Create Policies privilege but not the Update Feeds privilege, that user can create users with the Create Policies privilege, but not the Update Feeds privilege.
Organization	(Required) The organization where you want to assign the user account.
Group	(Required) The group where you want to assign the user account. A user's group determines their access to Tenable Security Center Director resources. For more information about groups, see Groups. To grant a user limited privileges to other groups' resources, see Custom Group Permissions.
Group Permissions	
Manage All Users	When enabled, allows the user to manage users in all of the user's assigned groups. For more information, see Custom Group Permissions.
Manage All Objects	When enabled, allows the user to manage objects in all of the user's assigned groups. For more information, see Custom Group Permissions.
Responsibility	
Asset	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.
Display Options	

Dark Mode	When enabled, sets the Tenable Security Center user interface to dark mode for the user.
Contact Information	
Title	The contact information for the user.
Address	
City	
State	
Country	
Email	
Phone	

SAML User Account Options

You must configure SAML authentication to add SAML-authenticated users. For more information, see SAML Authentication.

To add a SAML-authenticated user, see Add a SAML-Authenticated User.

Option	Description
First Name	The user's first name.
Last Name	The user's last name.
Type	(If LDAP or SAML are configured) The type of authentication you want to perform on the user: • Tenable (**TNS**)

	• Lightweight Directory Access Protocol (**LDAP**) • Security Assertion Markup Language (**SAML**) You must configure an LDAP server or SAML authentication in order to select **LDAP** or **SAML** from the **Type** drop-down box.
Username	(Required) The user's SAML username. Type the username exactly as it appears in your identity provider SAML configuration for this user.
Time Zone	(Required) The time zone for the user.
Scan Result Default Timeframe	The default **Completion Time** filter applied when the user accesses or refreshes the scan results page.
Cached Fetching	When enabled, Tenable Security Center Director caches plugin policy information and performs plugin policy downloads once per page load.
Membership	
Role	(Required) 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: • If a user is an Auditor, they can create new Auditors or lesser roles. • If a custom user has the Create Policies privilege but not the Update Feeds privilege, that user can create users with the Create Policies privilege, but not the Update Feeds privilege.
Organization	(Required) The organization where you want to assign the user account.

Group	(Required) The group where you want to assign the user account. A user's group determines their access to Tenable Security Center Director resources. For more information about groups, see Groups. To grant a user limited privileges to other groups' resources, see Custom Group Permissions.
Group Permissions	
Manage All Users	When enabled, allows the user to manage users in all of the user's assigned groups. For more information, see Custom Group Permissions.
Manage All Objects	When enabled, allows the user to manage objects in all of the user's assigned groups. For more information, see Custom Group Permissions.
Responsibility	
Asset	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.
Display Options	
Dark Mode	When enabled, sets the Tenable Security Center user interface to dark mode for the user.
Contact Information	

Title	The contact information for the user.
Address	
City	
State	
Country	
Email	
Phone	

LDAP Authentication

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

> **Note:** Tenable Security Center Director does not support SHA1 certificates for connecting to LDAP servers. Tenable Security Center Director uses OpenSSL3, which requires SHA256 certificates for authentication.

After you configure an LDAP server, create Tenable Security Center Director user accounts for each LDAP user you want to grant access.

- To manually add LDAP-authenticated users in Tenable Security Center Director, see Add an LDAP-Authenticated User.
- To automatically add LDAP-authenticated users by importing users from your LDAP identity provider, see LDAP User Provisioning.

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

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

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

Note: Tenable Security Center Director cannot retrieve more than one page of LDAP results. If Tenable Security Center 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 information on how to add or delete LDAP servers, see Manage LDAP Servers.

LDAP Authentication Options

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

Option	Description
Server Settings	
Name	(Required) A unique name for the LDAP server.
Description	A description for the LDAP server.
Hostname	(Required) The IP address or DNS name of the LDAP server.
Port	(Required) The remote LDAP port. Confirm the selection with your LDAP server administrators. • When **Encryption** is **None**, **Port** is typically **389**. • When **Encryption** is **TLS** or **LDAPS**, **Port** is typically **636**.
Encryption	If the LDAP server encrypts communications, the encryption method: Transport Layer Security (STARTTLS) or LDAP over SSL (LDAPS).

Option	Description
Username / Password	(Required) The username and password for an account on the LDAP server with credentials to search for user data. For example, Active Directory servers require an authenticated search. The following username formats are supported: • **Distinguished Name (DN)** – The RFC 4514-compliant DN format (for example, `CN=username,OU=OrgUnit,DC=example,DC=com`). This format works for both Active Directory and non-Active Directory LDAP servers (such as OpenLDAP). • **Domain\Username** – The standard Windows format (for example, `DOMAIN\username`). This format is specific to Active Directory servers. • **User Principal Name (UPN)** – The email-style format (for example, `username@example.com`). This format is available on Active Directory servers only when a UPN suffix has been configured in the Active Directory environment. Contact your LDAP server administrator to confirm which format your server requires. **Tip:** It is recommended to use passwords that meet stringent length and complexity requirements.
User Provisioning	You can enable user provisioning to automatically create LDAP-authenticated users in Tenable Security Center by importing user accounts from your LDAP identity provider. When user provisioning is enabled, users who log in to your LDAP identity provider are automatically created in Tenable Security Center.

Option	Description
	Tenable Security Center supports the following LDAP authentication systems for user provisioning: • Active Directory on Microsoft Server 2016 (on-premises) • Active Directory on Microsoft Server 2019 (on-premises) For more information, see LDAP User Provisioning. **Note:** If you want to delete a Tenable Security Center user that was created via LDAP user provisioning, delete the user from your LDAP identity provider. If you delete a user in Tenable Security Center that was created via LDAP user provisioning without deleting the user in your LDAP identity provider, Tenable Security Center automatically re-creates the user in Tenable Security Center the next time they log in using your LDAP identity provider.
User Data Sync	If you enable **User Provisioning**, you can enable **User Data Sync** to allow Tenable Security Center to automatically synchronize contact information (first name, last name, email address, and phone number) from your LDAP identity provider for Tenable Security Center users created via LDAP user provisioning. For more information, see LDAP User Provisioning. **Note:** If you want to edit a Tenable Security Center user that was created via LDAP user provisioning and you enabled **User Data Sync**, edit the user in your LDAP identity provider. Otherwise, the Tenable Security Center user data synchronization overwrites your changes the next time the user logs in to Tenable Security Center using your LDAP identity provider.
LDAP Schema Settings	
Base DN	(Required) The LDAP search base used as the starting point to search for the user data.

Option	Description
User Object Filter	The string you want to use to create a search based on a location or filter other than the default search base or attribute.
User Schema Settings (Optional, if you plan to use the LDAP server only as an LDAP query asset.)	
Username Attribute	The attribute name on the LDAP server that contains the username for the account. This is often specified by the string **sAMAccountName** in Active Directory servers that may be used by LDAP. Contact your LDAP server administrator for the correct value.
E-mail Attribute	The attribute name on the LDAP server that contains the email address for the account. This is often specified by the string **mail** in Active Directory servers that may be used by LDAP. Contact your LDAP server administrator for the correct value.
Phone Attribute	The attribute name on the LDAP server that contains the telephone number for the account. This is often specified by the string **telephoneNumber** in Active Directory servers that may be used by LDAP. Contact your LDAP server administrator for the correct value.
Name Attribute	The attribute name on the LDAP server that contains the name associated with the account. This is often specified by the string **CN** in Active Directory servers that may be used by LDAP. Contact your LDAP administrator for the correct value.
Access Settings	
Organizations	The Tenable Security Center Director organizations you want to authenticate using this LDAP server.

Option	Description
Advanced Settings	
Lowercase	When enabled, Tenable Security Center Director modifies the usernames sent by the LDAP server to use only lowercase characters. Tenable recommends keeping this option disabled.
DNS Field	The LDAP server parameter used in LDAP server requests to filter the returned asset data. Tenable recommends using the default value provided by Tenable Security Center Director.
Time Limit	The number of seconds you want Tenable Security Center Director to wait for search results from the LDAP server. Tenable recommends using the default value provided by Tenable Security Center Director.

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.

Manage LDAP Servers

Required Tenable Security Center User Role: Administrator

For more information about LDAP server options, see LDAP Authentication.

Add an LDAP Server

To add an LDAP server connection:

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, click **System** > **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 LDAP-authenticated user accounts.
    - To manually add LDAP-authenticated users in Tenable Security Center, see Add an LDAP-Authenticated User.
    - To automatically add LDAP-authenticated users by importing users from your LDAP identity provider, see Configure LDAP User Provisioning.

Delete an LDAP Server

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

To delete an LDAP server connection:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **System** > **LDAP Servers**.
3. Select the server connection you want to delete:

- To delete a single server connection:
    a. In the table, right-click the row for the server connection you want to delete.

       The actions menu appears.

    b. Click **Delete**.
- To delete multiple server connections:
    a. In the table, select the check box for each server connection you want to delete.

       The available actions appear at the top of the table.

    b. At the top of the table, click **Delete**.

  A confirmation window appears.

4. Click **Delete**.

   Tenable Security Center Director deletes the LDAP server.

LDAP User Provisioning

You can enable user provisioning to automatically create LDAP-authenticated users in Tenable Security Center by importing user accounts from your LDAP identity provider. When user provisioning is enabled, users who log in to your LDAP identity provider are automatically created in Tenable Security Center.

Tenable Security Center supports the following LDAP authentication systems for user provisioning:

- Active Directory on Microsoft Server 2016 (on-premises)
- Active Directory on Microsoft Server 2019 (on-premises)

For more information about LDAP authentication in Tenable Security Center, see LDAP Authentication.

If you enable user provisioning and a user who does not have a Tenable Security Center user account logs in using your LDAP identity provider, Tenable Security Center automatically creates a user account for them in Tenable Security Center.

Tenable Security Center creates users using data from attribute fields you map to the corresponding fields in your LDAP identity provider. If you enable **User Data Sync** for an LDAP server, each time a user logs into Tenable Security Center using your LDAP identity provider, Tenable Security Center updates any mapped attribute fields in Tenable Security Center with values from the fields in your LDAP identity provider. For more information about **User Data Sync**, see LDAP Authentication Options.

Note: If you want to edit a Tenable Security Center user that was created via LDAP user provisioning and you enabled **User Data Sync**, edit the user in your LDAP identity provider. Otherwise, the Tenable Security Center user data synchronization overwrites your changes the next time the user logs in to Tenable Security Center using your LDAP identity provider.

Note: If you want to delete a Tenable Security Center user that was created via LDAP user provisioning, delete the user from your LDAP identity provider. If you delete a user in Tenable Security Center that was created via LDAP user provisioning without deleting the user in your LDAP identity provider, Tenable Security Center automatically re-creates the user in Tenable Security Center the next time they log in using your LDAP identity provider.

For more information, see Configure LDAP User Provisioning.

Configure LDAP User Provisioning

Required Tenable Security Center User Role: Administrator

You can enable user provisioning to automatically create LDAP-authenticated users in Tenable Security Center by importing user accounts from your LDAP identity provider. When user provisioning is enabled, users who log in to your LDAP identity provider are automatically created in Tenable Security Center.

Tenable Security Center supports the following LDAP authentication systems for user provisioning:

- Active Directory on Microsoft Server 2016 (on-premises)
- Active Directory on Microsoft Server 2019 (on-premises)

For more information, see LDAP User Provisioning.

To manually create LDAP-authenticated users in Tenable Security Center, see Add an LDAP-Authenticated User.

For more information about user account configuration options, see LDAP User Account Options.

Before you begin:

1. (Recommended) Create a backup of your user directory in your LDAP identity provider.
2. In Tenable Security Center, add an LDAP server, as described in Manage LDAP Servers.
3. In your LDAP identity provider, create the following custom user attributes: tenableRoleID, tenableGroupID, and tenableOrgID.
4. In your LDAP identity provider, specify the role, group, and organization you want to assign the user in Tenable Security Center:
    a. In the tenableRoleID attribute field, type the ID for the Tenable Security Center role you want to assign to the user. To locate the ID for a role, see View User Role Details.
    b. In the tenableGroupID attribute field, type the ID for the Tenable Security Center group you want to assign to the user. To locate the ID for a group, see View Group Details.
    c. In the tenableOrgID attribute field, type the ID for the Tenable Security Center organization you want to assign to the user. To locate the ID for an organization, see View Organization Details.

To enable LDAP user provisioning for an LDAP server:

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, click **Resources** > **LDAP Servers**.

    The **LDAP Servers** page appears.
3. Right-click the row for the LDAP server where you want to enable user provisioning.

    The actions menu appears.

    -or-

    Select the check box for the LDAP server where you want to enable user provisioning.

    The available actions appear at the top of the table.

4. Click **Edit**.

   The **Edit LDAP Server** page appears.

5. In the **Server Settings** section, click the toggle to enable **User Provisioning**.
6. (Optional) To automatically update contact information (first name, last name, email address, and phone number) for users created via LDAP user provisioning, click the **User Data Sync** toggle. For more information about **User Data Sync**, see LDAP Authentication Options.
7. (Optional) In the **User Schema Settings** section, type the names of the attributes in your LDAP identity provider you want to use to populate the **Username**, **Email**, **Phone**, **First Name**, and **Last Name** for users created via LDAP user provisioning. For more information about user account options, see LDAP User Account Options.

   > **Note:** If you enable **User Data Sync** and configure the options in the **User Schema Settings** section, Tenable Security Center automatically updates the attributes in the **User Schema Settings** section with values from your LDAP identity provider. For more information, see LDAP Authentication Options.

8. Click **Submit**.

   Tenable Security Center Director saves your configuration.

LDAP Servers with Multiple OUs

Tenable's Tenable Security Center 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 Security Center 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 Security Center Director via the user interface.
2. Click **Resources** > **LDAP Servers**.
3. Add the LDAP server, as described in Manage LDAP Servers.

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

4. Log out of Tenable Security Center Director.
5. Log in to Tenable Security Center 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.

   In the **Search String** box, type **=***.

Option 2

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

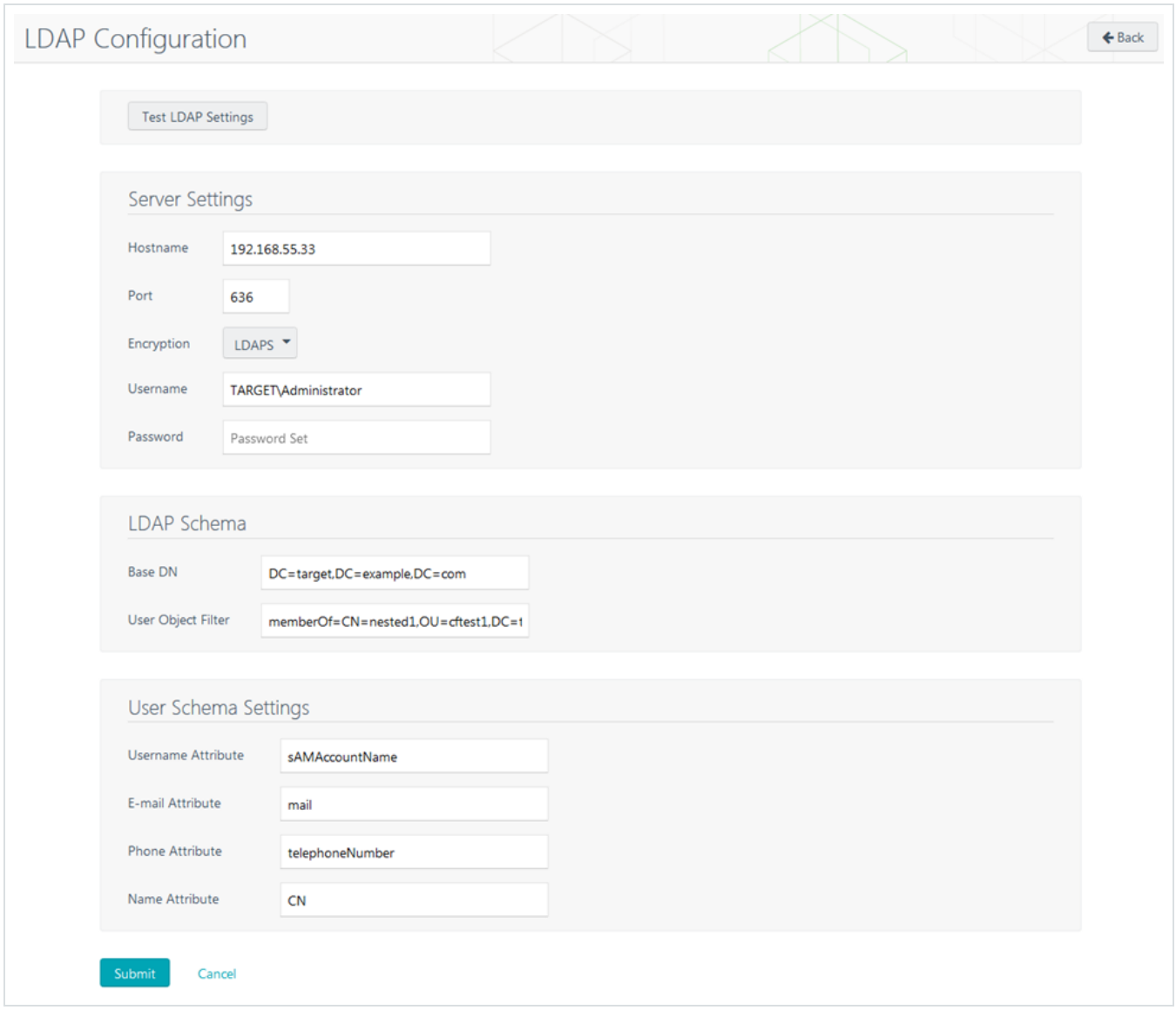
The example above could be used along with a **Search String** for global usage. As another example, you might use this search string, when used in the configuration, applies to all LDAP searches:

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 Security Center Director via the user interface.
2. Click **Resources** > **LDAP Servers**.
3. Begin configuring the LDAP server, as described in Manage LDAP Servers.



4. Click **Test LDAP Settings** to test configurations.
5. Log out of Tenable Security Center Director.
6. Log in to Tenable Security Center 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.

   In the **Search String** box, type **=***.

SAML Authentication

You can configure SAML authentication so that Tenable Security Center Director users can use identity provider-initiated single sign-on (SSO) when logging in to Tenable Security Center Director. Tenable Security Center Director supports SAML 2.0-based authentication (for example, Okta, OneLogin, Microsoft ADFS, or Shibboleth 2.0).

For more information, see:

- Tenable SAML Configuration Quick-Reference Guide
- 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 Security Center Director user accounts for each SAML user you want to grant access.

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

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

Considerations for Advanced SAML Features

Tenable Security Center Director uses the open-source SimpleSAMLphp library for SAML authentication. Tenable Security Center Director supports standard SAML 2.0 authentication but

does not support SAML assertion encryption. If you want to configure SAML authentication, choose an identity provider that does not require assertion encryption and confirm that assertion encryption is not enabled. For information about Tenable Security Center Director communications encryption, see Encryption Strength.

Signatures. Configure your identity provider to use the RSA-SHA256, RSA-SHA384, or RSA-SHA512 signature algorithm. Do not use RSA-SHA1 or ECDSA signature algorithms. At least one of the SAML response or the SAML assertion must be signed. If your identity provider supports it, Tenable recommends signing both.

Time synchronization. Configure the time source for the Tenable Security Center Director host and your identity provider using the same time service, such as NTP. If the time on either system differs beyond the allowed tolerance, authentication fails with an error similar to `IssueInstant is not within bounds`.

Single logout. Tenable Security Center Director does not initiate single logout (SLO). Logging out of Tenable Security Center Director ends only your Tenable Security Center Director session and does not log you out of your identity provider. Configure session timeouts in your identity provider to meet your requirements. If your identity provider does not support single logout, leave the **Single Logout Service** field blank or enter a placeholder value.

> **Note:** The **Single Logout Service** field does not affect authentication. Tenable Security Center Director does not send logout requests to your identity provider.

Logging in. Users log in to Tenable Security Center Director using the **Sign In Using Identity Provider** button, as described in Log In to the Web Interface. After logging in, direct links to dashboards or reports redirect you to the default page. Re-open the link after you log in.

User identification. By default, Tenable Security Center Director uses the SAML NameID as the username. To use a different assertion attribute, type the attribute name in the **Username Attribute** box. The attribute name is case-sensitive and must match exactly as it appears in your identity provider SAML configuration. You can use any attribute, such as `displayName`, `userPrincipalName`, or `sAMAccountName`. Tenable Security Center Director uses the first value of the attribute.

User provisioning attributes. If you enable user provisioning, your identity provider must send the following attributes in the SAML assertion. Type the attribute names exactly as they appear in your identity provider configuration.

Tenable Security Center Director Field	Attribute Name	Value
Organization ID	`tenableOrgID`	The numeric organization ID displayed in Tenable Security Center Director
Group ID	`tenableGroupID`	The numeric group ID displayed in Tenable Security Center Director
Role ID	`tenableRoleID`	The numeric role ID displayed in Tenable Security Center Director. If the role is Administrator, the Organization ID must be 0

You can also send the following optional attributes: `tenableFirstName`, `tenableLastName`, `tenableTitle`, `tenableEmail`, `tenableAddress`, `tenableCity`, `tenableState`, `tenablePhone`, `tenableCountry`, and `tenableTimezone`. For `tenableTimezone`, use a time zone identifier such as `America/New_York`. Each organization, group, and role assignment is applied when Tenable Security Center Director provisions the user. Tenable Security Center Director does not re-evaluate these assignments when the user logs in again. If you enable user data sync, Tenable Security Center Director updates contact information at each login.

Identity provider certificates. Updating the identity provider signing certificate does not require you to restart Tenable Security Center Director. Import your identity provider metadata again or update the certificate data in the SAML configuration. The new certificate takes effect the next time a user logs in. Tenable Security Center Director stores a single certificate. Complete your identity provider certificate rollover before you update the certificate in Tenable Security Center Director.

Backing up SAML configuration. A full backup and restore to a new host retains your SAML configuration. The host name or IP address of the new host does not affect your SAML configuration.

Advanced configuration. Tenable Security Center Director regenerates its SAML configuration files when you change the SAML configuration. Do not edit these files directly. To configure SAML options that are not available in the interface, use the configuration override files `authsources-custom.php` and `saml20-idp-remote-custom.php`, located in the same directories. For more information, see Using a Custom entityID with Tenable Security Center SAML.

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

SAML Authentication Options

Option	Description
SAML	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 Security Center.
Source	Specifies your SAML configuration method: • **Import** – Configure SAML authentication by uploading the metadata file provided by your identity provider, as described in Configure SAML Authentication Automatically via the User Interface. • **Entry** – Configure SAML authentication by manually configuring SAML options using data from the metadata file provided by your identity provider, as described in Configure SAML Authentication Manually via the User Interface.
Type	Specifies the identity provider you are using: **SAML 2.0** (e.g., Okta,

Option	Description
	OneLogin, Shibboleth 2.0, etc.).
Entity ID	The name of the Entity ID attribute. Type the attribute exactly as it appears in your identity provider SAML configuration. The Entity ID must be in URL format. **Tip:** This is the **Federation Service Identifier** value in Microsoft ADFS.
Identity Provider (IdP)	The identity provider identifier string. For example: • The **Identity Provider Issuer** value in Okta. • The **Federation Service Identifier** value in Microsoft ADFS.
Username Attribute	The name of the SAML username attribute. Type the attribute exactly as it appears in your identity provider SAML configuration. For example, if your SAML username attribute is **NameID**, specify **NameID** to instruct Tenable Security Center to recognize users who match the format `NameID=`*`username`*.
Single Sign-on Service	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.
Single Logout Service	The identity provider URL where users log out. Type the URL exactly as it appears in your identity provider SAML metadata.
Certificate Data	The text of the identity provider's X.509 SSL certificate, without the `===BEGIN CERT===` and the `===END CERT===` strings.
User Provisioning	You can enable user provisioning to automatically create SAML-authenticated users in Tenable Security Center Director by importing user

Option	Description
	accounts from your SAML identity provider. When user provisioning is enabled, users who log into your SAML identity provider are automatically created in Tenable Security Center Director. For more information, see SAML User Provisioning. **Note:** If you want to delete a Tenable Security Center user that was created via SAML user provisioning, delete the user from your SAML identity provider. If you delete a user in Tenable Security Center that was created via SAML user provisioning without deleting the user in your SAML identity provider, Tenable Security Center automatically re-creates the user in Tenable Security Center the next time they log in using your SAML identity provider.
User Data Sync	If you enabled **User Provisioning**, you can enable **User Data Sync** to allow Tenable Security Center to automatically synchronize contact information from your SAML identity provider for Tenable Security Center users created via SAML user provisioning. For more information, see SAML User Provisioning. **Note:** If you want to edit a Tenable Security Center user that was created via SAML user provisioning and you enabled **User Data Sync**, edit the user in your SAML identity provider. Otherwise, the Tenable Security Center user data sync overwrites your changes the next time the user logs in to Tenable Security Center using your SAML identity provider. **Note:** Tenable Security Center 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.

Configure SAML Authentication Automatically via the User Interface

Required Tenable Security Center User Role: Administrator

You can use this method to configure most types of SAML authentication via the Tenable Security Center Director user interface. If you encounter issues with this method (for example, 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:

- Review the Tenable SAML Configuration Quick-Reference guide for a step-by-step guide of how to configure SAML for use with Tenable Security Center Director.
- Save your identity provider SAML metadata file to a directory on your local computer.

To automatically configure SAML authentication for Tenable Security Center Director users:

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, 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 Security Center 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, Shibboleth 2.0, etc.).
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 Security Center Director rejects the file, contact your identity provider for assistance.

8. Click **Submit**.

   Tenable Security Center 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 Security Center 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 Security Center 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 Tenable Security Center User Role:** Administrator

You can use this method to configure most types of SAML authentication via the Tenable Security Center 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 (for example, 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:

- Review the Tenable SAML Configuration Quick-Reference guide for a step-by-step guide of how to configure SAML for use with Tenable Security Center Director.
- Save your identity provider SAML metadata file to a directory on your local computer.

To configure SAML authentication for Tenable Security Center Director users:

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, 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 Security Center 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, Shibboleth 2.0, etc.).
   b. In the **Entity ID** box, type the name of the Entity ID attribute exactly as it appears in your identity provider SAML configuration. The **Entity ID** must be in URL format.
   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. This field is case-sensitive.
   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 Security Center 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 Security Center 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 Security Center 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 Tenable Security Center User Role: Administrator

Note: These instructions are not for general configuration. These steps should be used only by advanced users or for custom configuration. The recommended method for configuring SAML authentication is via the Tenable Security Center interface:

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

Note: Tenable Security Center Director regenerates the `authsources.php` and `saml20-idp-remote.php` files each time you change the SAML configuration. Do not edit these files directly. Use the `authsources-custom.php` and `saml20-idp-remote-custom.php` override files, located in the same directories. For more information, see Using a Custom entityID with Tenable Security Center SAML.

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

For general information, see SAML Authentication.

Before you begin:

- Review the Tenable SAML Configuration Quick-Reference guide for a step-by-step guide of how to configure SAML for use with Tenable Security Center Director.
- 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 Security Center Director via the user interface.
2. In the left navigation, 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 Security Center Director saves your configuration.
6. Log in to Tenable Security Center Director via the command line interface (CLI).
7. Navigate to and open the `/opt/sc/support/etc/SimpleSAML/config/authsources-custom.php` file.
8. Copy and paste the following text into the file, between the `),` line and the `);` line:

```
// 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.
```

```
'core:AdminPassword',
),
```

9. Save the file.
10. Navigate to and open the `/opt/sc/support/etc/SimpleSAML/config/config.php` file.

    Note: By default, SimpleSAML uses `Security Center` for the technical contact name (`technicalcontact_name`) and `noreply@localhost` for the technical contact email address (`technicalcontact_email`). SimpleSAML uses the email address as the recipient of error reports and as the technical contact in generated metadata.

11. Copy and paste the following text into the file to enable the admin module:

```
'module.enable' => [
'admin' => true,
],
```

12. Save the file.
13. In a browser, navigate to **https://<*Tenable Security Center IP address or hostname*>/saml/module.php/core/frontpage_config.php**.

    The **SimpleSAML.php installation** page appears.
14. On the **Configuration** tab, click **Login as administrator**.

    The **Enter your username and password** page appears.
15. In the **Username** box, type *admin*.
16. In the **Password** box, type *admin*.
17. Click **Login**.
18. On the **Federation** tab, in the **Tools** section, click **XML to SimpleSAML.php metadata converter**.

    The **Metadata parser** page appears.
19. Click **Choose File** and select your identity provider SAML metadata file.
20. Click **Parse**.

Tenable Security Center Director validates the identity provider SAML metadata file. If the metadata file is supported, Tenable Security Center 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 Security Center Director.

21. In the **saml20-idp-remote** section, copy the text in the box.
22. Log in to Tenable Security Center Director via the command line interface (CLI).
23. Navigate to and open the `/opt/sc/support/etc/SimpleSAML/metadata/saml20-idp-remote-custom.php` file (for SAML 2.0 or Shibboleth 2.0).
24. Paste the text into the file, after the `<?php` line.
25. Save the file.
26. Navigate to and open the `/opt/sc/support/etc/SimpleSAML/config/authsources-custom.php` file again.
27. Confirm the **idp** URL in the `authsources-custom.php` file matches the **$metadata** URL in the `saml20-idp-remote-custom.php` or `shib13-idp-remote.php` file:

    Valid `authsources-custom.php` syntax example:

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

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

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

28. In a browser, navigate to **https://<*Tenable Security Center IP address or hostname*>/saml/module.php/core/frontpage_config.php**.

    The **SimpleSAML.php installation** page appears.
29. On the **Authentication** tab, click **Test configured authentication sources**.

    The **Test authentication sources** page appears.
30. Click **1**.

    Your identity provider login page appears.

31. 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 Security Center interface, on the **SAML Configuration** page, 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 Security Center 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 Security Center Director using the **Sign In Using Identity Provider** button, as described in Log In to the Web Interface.

SAML User Provisioning

You can enable user provisioning to automatically create SAML-authenticated users in Tenable Security Center 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 Security Center Director. For more information about SAML authentication in Tenable Security Center, see SAML Authentication.

> **Tip:** Review the Tenable SAML Configuration Quick-Reference guide for a step-by-step guide of how to configure SAML for use with Tenable Security Center Director.

If you enable user provisioning and a user who does not have a Tenable Security Center Director user account logs in using your SAML identity provider, Tenable Security Center Director automatically creates a user account for them in Tenable Security Center Director.

Tenable Security Center 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 Security Center Director using your SAML identity provider, Tenable Security Center Director updates any mapped attribute fields in Tenable Security Center Director with values from the fields in your SAML identity provider. For more information about **User Data Sync**, see SAML Authentication Options.

Note: If you want to edit a Tenable Security Center user that was created via SAML user provisioning and you enabled **User Data Sync**, edit the user in your SAML identity provider. Otherwise, the Tenable Security Center user data sync overwrites your changes the next time the user logs in to Tenable Security Center using your SAML identity provider.

Note: If you want to delete a Tenable Security Center user that was created via SAML user provisioning, delete the user from your SAML identity provider. If you delete a user in Tenable Security Center that was created via SAML user provisioning without deleting the user in your SAML identity provider, Tenable Security Center automatically re-creates the user in Tenable Security Center the next time they log in using your SAML identity provider.

For more information, Configure SAML User Provisioning.

Configure SAML User Provisioning

Required Tenable Security Center User Role: Administrator

You can enable user provisioning to automatically create SAML-authenticated users in Tenable Security Center 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 Security Center Director. For more information, see SAML User Provisioning.

To manually create SAML-authenticated users in Tenable Security Center Director, see Add a SAML-Authenticated User.

For more information about user account configuration options, see SAML User Account Options.

Before you begin:

- Review the Tenable SAML Configuration Quick-Reference guide for a step-by-step guide of how to configure SAML for use with Tenable Security Center Director.
- 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 Security Center Director via the user interface.
2. In the left navigation, 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. For more information about **User Data Sync**, see SAML Authentication Options.
6. Click **Submit**.

   Tenable Security Center Director saves your configuration.

What to do next:

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

  For the attribute names and values your identity provider must send, see User provisioning attributes. If you enable user provisioning, your identity provider must send the following attributes in the SAML assertion. Type the attribute names exactly as they appear in your identity provider configuration..

  > **Note:** Tenable Security Center Director uses the fields listed in the **Attribute Mapping** section to create and update users in Tenable Security Center Director. Any Tenable fields that you map to corresponding fields in your SAML identity provider populate when Tenable Security

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

SAML Authentication XML Configuration Examples

Tip: Review the Tenable SAML Configuration Quick-Reference guide for a step-by-step guide of how to configure SAML for use with Tenable Security Center Director.

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

OneLogin Example

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

OneLogin Field	Description
Relay State	Leave this field blank.
Audience	Type `https://tenable.sc`.
Recipient	Type `https://<Tenable Security Center host>/saml/module.php/saml/sp/saml2-acs.php/1`, where *<Tenable Security Center host>* is the IP address or hostname for Tenable Security Center Director.
ACS (Consumer) URL Validatior	Type `-*`.
ACS	Type `https://<Tenable Security Center`

OneLogin Field	Description
(Consumer) URL	*host*>/saml/module.php/saml/sp/saml2-acs.php/1, where *<Tenable Security Center host>* is the IP address or hostname for Tenable Security Center Director.
Single Logout URL	Type https://*<Tenable Security Center host>*/saml/module.php/saml/index.php?sls, where *<Tenable Security Center host>* is the IP address or hostname for Tenable Security Center Director.

Okta Example

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

Okta Field	Description
General	
Single Sign On URL	Type https://*<Tenable Security Center host>*/saml/module.php/saml/sp/saml2-acs.php/1, where *<Tenable Security Center host>* is the IP address or hostname for Tenable Security Center Director.
Recipient URL	Type https://*<Tenable Security Center host>*/saml/module.php/saml/sp/saml2-acs.php/1, where *<Tenable Security Center host>* is the IP address or hostname for Tenable Security Center Director.
Destination URL	Type https://*<Tenable Security Center host>*/saml/module.php/saml/sp/saml2-acs.php/1, where *<Tenable Security Center host>* is the IP address or hostname for Tenable Security Center Director.

Okta Field	Description
Audience Restriction	Type `https://tenable.sc`.
Default Relay State	Leave this field blank.
Name ID Format	Set to `Unspecified`.
Response	Set to `Signed`.
Assertion Signature	Set to `Signed`.
Signature Algorithm	Set to `RSA_SHA256`.
Digest Algorithm	Set to `SHA256`.
Assertion Encryption	Set to `Unencrypted`.
SAML Single Logout	Set to `Disabled`.
authnContextClassRef	Set to `PasswordProtectedTransport`.
Honor Force Authentication	Set to `Yes`.
SAML Issuer ID	Type `http://www.okta.com/${org.externalKey}`.
Attribute Statements	
FirstName	Set to **Name Format:** `Unspecified` and **Value:** `user.firstName`.
LastName	Set to **Name Format:** `Unspecified` and **Value:** `user.lastName`.
Email	Set to **Name Format:** `Unspecified` and **Value:** `user.email`.
username	Set to **Name Format:** `Unspecified` and one of the following:

Okta Field	Description
	• **Value:** `user.displayName`, if your Tenable Security Center Director user account usernames are full names (e.g., Jill Smith). • **Value:** `user.email`, if your Tenable Security Center Director user account usernames are email addresses (e.g., jsmith@website.com). • **Value:** `user.login`, if your Tenable Security Center Director user account usernames are name-based text strings (e.g., jsmith).

Microsoft ADFS Example

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

Microsoft ADFS Configuration	Description
Edit Authentication Methods window	
Extranet	Select, at minimum, the **Forms Authentication** check box.
Intranet	Select, at minimum, the **Forms Authentication** check box.
Add Relying Party Trust wizard	
Welcome section	• Select **Claims aware**. • Select **Import data about the relying party from a file**. • Browse to and select the SAML configuration `.xml` file you downloaded from Tenable Security Center Director.

Microsoft ADFS Configuration	Description
	Note: If you see a warning that some content was skipped, click **Ok** to continue.
Specify Display Name section	In the **Display Name** box, type your Tenable Security Center Director FQDN.
Configure Certificate section	Browse to and select the encryption certificate you want to use.
Choose Access Control Policy section	Select the **Permit everyone** policy.
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 Security Center 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**.

Microsoft ADFS Configuration	Description
	3. In **Outgoing name ID format**, select **Transient Identifier**. 4. Select the **Pass through all claim values** check box. **Note:** If you select **Transient Identifier**, your identity provider sends a different NameID value for each login. In Tenable Security Center Director, set the **Username Attribute** to the claim that contains the email address or UPN. If you leave the **Username Attribute** set to NameID and enable user provisioning, each login appears as a new user. **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.

SSL Client Certificate Authentication

Note: Tenable has validated certificate support for Signature Algorithms up to SHA-384 and RSA key sizes of up to 4096 bits.

You can use configure SSL client certificate authentication for Tenable Security Center Director user account authentication. Tenable Security Center 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 Security Center Director user accounts:

1. Configure Tenable Security Center Director to allow SSL client certificate authentication, as described in Configure Tenable Security Center Director to Allow SSL Client Certificate Authentication.
2. Configure Tenable Security Center 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 Security Center Director, as described in Configure a CRL in Tenable Security Center Director or Configure OCSP Validation in Tenable Security Center Director.

What to do next:

- Instruct users to log in to Tenable Security Center Director via certificate, as described in Log in to the Web Interface via SSL Client Certificate.

Configure Tenable Security Center Director to Allow SSL Client Certificate Authentication

You must configure the Tenable Security Center Director server to allow SSL client certificate connections. For complete information about certificate authentication, see SSL Client 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:

Value	Description
none (default)	Tenable Security Center Director does not accept SSL certificates for user authentication.
require	Tenable Security Center Director requires a valid SSL certificate for user authentication.
optional	Tenable Security Center Director accepts but does not require a valid SSL certificate for user authentication. If a user does not present a certificate, they can log in via username and password. **Note:** Some browsers may not connect to Tenable Security Center when you use the **optional** setting.
optional_no_ca	Tenable Security Center Director accepts valid and invalid SSL certificates for user authentication. **Tip:** This setting does not configure reliable user authentication, but you can use it to troubleshoot issues with your SSL connection and determine whether there is an issue with the key or the CA.

3. Edit the **SSLVerifyDepth** setting to specify the length of the certificate chain you want Tenable Security Center Director to accept for user authentication. For example:
    - When set to **0**, Tenable Security Center Director accepts self-signed certificates.
    - When set to **1**, Tenable Security Center Director does not accept intermediate certificates. Tenable Security Center Director accepts self-signed certificates or certificates signed by known CAs.
    - When set to **2**, Tenable Security Center Director accepts up to 1 intermediate certificate. Tenable Security Center 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 Security Center Director saves your configuration.

Configure a CRL in Tenable Security Center Director

> **Required Tenable Security Center User Role:** Root user

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

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

Before you begin:

- Confirm that you have the `mod_ssl` Apache module installed on Tenable Security Center 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 Security Center 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 Security Center Director saves your configuration.
2. Restart Tenable Security Center Director, as described in Start, Stop, or Restart Tenable Security Center Director.

Tenable Security Center Director restarts.

3. Confirm that your CA root configuration file contains the following parameters:

   - `crl_dir`
   - `database`
   - `crl`
   - `clr_extensions`
   - `default_crl_days`

   For example:

```
...
# 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 Security Center Director in a subdirectory of `/opt/sc/support/conf/`.
6. Configure Tenable Security Center Director to trust your CA, as described in Trust a Custom CA.

   Tenable Security Center Director processes your CA.

7. In the command line interface (CLI), run the following command to enable the CRL in Tenable Security Center Director:

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

   For example:

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

   Tenable Security Center 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:

Content	Description
SSLCARevocationCheck <*value*>	
chain	Tenable Security Center Director checks all certificates in a chain against the CRL.
leaf	Tenable Security Center Director checks only the end-entity certificate in a chain against the CRL.
SSLCARevocationFile <*filepath*>	

Content	Description
Specifies the file path for the CRL file in Tenable Security Center Director. For example, `/opt/sc/support/conf/crl/ca.crl`.	

b. Save the file.

Tenable Security Center Director saves your configuration.

9. In the CLI, 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 Security Center Director creates a symbolic link for the CRL file.

10. Restart Tenable Security Center Director, as described in Start, Stop, or Restart Tenable Security Center Director.

Tenable Security Center Director restarts.

Configure OCSP Validation in Tenable Security Center Director

Required Tenable Security Center User Role: Root user

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

Note: Tenable Support does not assist with OCSP configuration in Tenable Security Center Director.

Before you begin:

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

To configure OCSP validation in Tenable Security Center 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 Security Center 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 Security Center Director saves your configuration.
3. Restart Tenable Security Center Director, as described in Start, Stop, or Restart Tenable Security Center Director.

   Tenable Security Center Director restarts.

Search

In Tenable Security Center, you can search for vulnerabilities (by CVE ID) and host assets (by IPv4 address) using the search box in the top navigation bar. Click the drop-down to change the category.

A list of suggestions appears after you type at least five characters or the first octet of an IPv4 address.

> **Note:** To search for host assets, you must have the **View Host Assets** permission enabled. For more information, see User Roles.

Tenable Security Center saves your search history. To view your search history, click the search box. To delete an item from your search history, click the ✕ icon next to the search term.

To view a search result, press **Enter** or click a suggestion in the drop-down box. The search results page appears, which displays widgets with details about the vulnerability or host asset:

Widget	Description
Vulnerabilities	
Vulnerability Information	A list of solutions for the vulnerability that correspond to the plugins currently visible in the **Tenable Coverage** widget. The top right corner displays the Vulnerability Priority Rating (VPR) for the vulnerability. For more information about VPRs, see CVSS vs. VPR.
VPR Key Drivers	Details about the history and severity of the vulnerability that contribute to the VPR. For more information about VPRs, see CVSS vs. VPR.
Risk Information	Details about the risk associated with the vulnerability, as determined by the National Vulnerability Database (NVD).
Hosts Impacted	A list of assets in your system that are affected by the vulnerability. When you scan your network, any discovered assets that are affected by the vulnerability will appear in this list. If you have a Tenable Security Center+ license, this widget also displays the

Widget	Description
	Asset Exposure Score (AES) and Asset Criticality Rating (ACR) for the assets. Click **More Details** to see the **IP Summary** page, where you can view the list of hosts filtered by the CVE ID.
CPEs	A list of CPE names that are relevant to the vulnerability. Click **More Details** to open a dialog box with the full list of CPEs.
References	A list of links with information relevant to the vulnerability. Click **More Details** to open a dialog box with the full list of references.
Tenable Coverage	A list of Tenable plugins that address the vulnerability. You can sort this list by plugin ID. When you sort plugins or navigate pages in the widget, the **Vulnerability Information** and **Related Links** widgets update to correspond to the visible plugins. Click **More Details** to see the **Vulnerability List** page, where you can view the list of plugins filtered by your assets. If none of the assets in your network are affected by the list of plugins, then this page will not display any plugins.
Related Links	A list of links with information relevant to the plugins currently visible in the **Tenable Coverage** widget. Click **More Details** to open a dialog box with the full list of related links.
Host Assets	

Widget	Description
Repository	The repository associated with the host asset. If the host asset appears in more than one repository, click the drop-down to view the host asset in a different repository.
Host Information	Details about the host asset. If you have a Tenable Security Center+ license, this widget also displays the Asset Exposure Score (AES) and Asset Criticality Rating (ACR) for the assets. Click **More Details** to open a dialog box with the full list of host details.
Host Vulnerability Severity	A chart that displays a breakdown of vulnerabilities by severity level.
Assets	A list of assets associated with the host.
Findings	A list of vulnerabilities in your system that correspond to the asset. When you scan your network, any vulnerabilities associated with the host asset will appear in this list. Click **More Details** to see the **Vulnerability List** page, where you can view the list of vulnerabilities filtered by the host asset.

Certificates and Certificate Authorities in Tenable Security Center Director

Tenable Security Center Director includes the following defaults:

- a default Tenable Security Center server certificate (`SecurityCenter.crt`)
- a Tenable Security Center 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 Security Center Director Server Certificates
- Trust a Custom CA
- SSL Client Certificate Authentication
- Custom Plugin Packages for NASL and CA Certificate Upload

Tenable Security Center Director Server Certificates

Tenable Security Center Director ships with a default Tenable Security Center 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 Tenable Nessus or your browser.

Problem	Solution
The default certificate for Tenable Security Center Director is untrusted.	Upload a certificate for theTenable Security Center Director server, as described in Upload a Server Certificate for Tenable Security Center. If the new server certificate is self-signed, plugin 51192 may report that the Tenable Security Center Director server certificate is untrusted. To configure Tenable Nessus to trust the server certificate, upload the CA certificate to Tenable Nessus.
Your browser reports	Upload a CA certificate for the Tenable Security Center Director

Problem	Solution
that the Tenable Security Center Director server certificate is untrusted.	server certificate to your browser.
Plugin 51192 reports that the Tenable Security Center Director server certificate expired.	Regenerate the Tenable Security Center Director server certificate, as described in Regenerate the Tenable Security Center Director Server Certificate.

Upload a Server Certificate for Tenable Security Center

Required Tenable Security Center User Role: Root user

For information about Tenable Security Center Director server certificates, see Tenable Security Center Director Server Certificates.

Note: When uploading a certificate file to Tenable Security Center Director, you must use a PEM file. 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 Security Center Director:

1. 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
```

2. 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.

3. To confirm the files have the correct permissions (600) and ownership (tns), run:

```
# ls -l /opt/sc/support/conf/SecurityCenter.crt
-rw-r----  1 tns tns  4389 May 15 15:12 SecurityCenter.crt
# ls -l /opt/sc/support/conf/SecurityCenter.key
-rw-r----  1 tns tns   887 May 15 15:12 SecurityCenter.key
```

   Note: If an intermediate certificate is required, it must also be copied to the system and given the correct permissions (600) 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:

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

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

   b. To change the permissions, run:

```
# chmod 600 /opt/sc/support/conf/SecurityCenter.crt
# chmod 600 /opt/sc/support/conf/SecurityCenter.key
```

4. Restart the Tenable Security Center Director service:

```
# service SecurityCenter restart
```

5. In a browser, log in to the Tenable Security Center Director user interface as a user with administrator permissions.
6. 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 Tenable Nessus.

Regenerate the Tenable Security Center Director Server Certificate

Required Tenable Security Center User Role: `tns` user

Required Tenable Security Center User Role: Root user

Tenable Security Center 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 Security Center Director SSL certificate:

1. Log in to Tenable Security Center Director via the command line interface (CLI).
2. In the CLI in Tenable Security Center Director, run the following command to switch to the `tns` user:

```
su - tns
```

3. As the `tns` user, run the following command:

```
/opt/sc/support/bin/php /opt/sc/src/tools/installSSLCertificate.php -h <IP|host name>
```

Note: The `-h` argument is required. Provide the IP address or hostname that clients use to access Tenable Security Center Director. This value is set as the Common Name for the new certificate.

(Optional) Include the argument `-q` to suppress the warning: `This script generates a self-signed SSL certificate, which is not recommended for production.`

Note: Tenable Security Center Director recommends running this command as the `tns` user, as shown above. If you run the command as the root user instead, you must ensure `/opt/sc/support/lib` is included in the `LD_LIBRARY_PATH` environment variable.

If the script completes without errors, Tenable Security Center Director has generated a new certificate. If the script reports an error, verify that you provided a valid IP address or hostname with the `-h` argument and that you are running the command as the `tns` user.

4. Run the following command to exit the `tns` user:

```
exit
```

5. As the root user, run the following command to restart the Tenable Security Center Director service:

```
# service SecurityCenter restart
```

The service restarts and Tenable Security Center Director applies the new certificate.

Note: After the service restarts, your browser may still display the old or expired certificate until you clear the browser cache or close and reopen the browser tab.

6. (Optional) Verify the new certificate is in place by running the following command to check the certificate dates:

```
openssl x509 -in /opt/sc/support/conf/SecurityCenter.crt -noout -dates
```

The output shows the `notBefore` and `notAfter` dates for the certificate. Confirm that `notBefore` reflects today's date and `notAfter` is two years in the future.

Trust a Custom CA

Required Tenable Security Center User Role: `tns` user

You can configure Tenable Security Center Director to trust a custom CA for certificate authentication or other uses. Common reasons to trust a custom CA include:

- Your organization uses an internal certificate authority to sign TLS certificates, and Tenable Security Center Director must connect to services signed by that CA.
- Your network uses an SSL inspection proxy that re-signs traffic with a corporate CA.
- You are configuring certificate-based user authentication. For more information, see SSL Client Certificate Authentication.

To configure Tenable Security Center Director to trust a custom CA:

1. Log in to Tenable Security Center Director via the user interface.
2. Copy the required PEM-encoded CA certificate (and intermediate CA certificate, if needed) to the Tenable Security Center Director server's `/tmp` directory. In this example, the file is named `ROOTCA2.cer`.

   Note: If you upload multiple certificates, upload each certificate individually in Privacy-Enhanced Mail (PEM) format. You must also upload certificate chain files individually in PEM format.

   PEM-encoded files begin with `-----BEGIN CERTIFICATE-----`. If your certificate file is in DER format (binary), convert it to PEM before proceeding:

   ```
   openssl x509 -inform DER -in ROOTCA2.cer -out ROOTCA2.pem
   ```

   Then use the converted `.pem` file in the following steps.

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 Security Center Director processes all the CAs in the file.

4. Restart Tenable Security Center Director, as described in Start, Stop, or Restart Tenable Security Center Director.

5. (Optional) Verify the CA was installed by confirming the certificate files exist in `/opt/sc/data/CA/`:

   ```
   ls /opt/sc/data/CA/
   ```

   The directory should contain the CA files created by the `installCA.php` script. If the files are not present, re-run the script and check for error output.

System Settings

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

- Configuration Settings
- Diagnostics Settings
- Job Queue Events
- System Logs
- Publishing Sites Settings
- Keys Settings
- User Profile Menu Settings

Configuration Settings

The **Configuration** menu contains settings for managing data retention, external communication, and system security.

Data Expiration Settings

Data expiration determines how long Tenable Security Center retains closed tickets, scan results, and report results.

Option	Description
User Generated Object Lifetime	
Closed Tickets	The number of days Tenable Security Center retains closed tickets. The default value is *365* days.
Report Results	The number of days Tenable Security Center retains report results. The default value is *365* days.
Tenable Security Center Instance Data Lifetime	
Scan Results	The number of days Tenable Security Center Director retains scan results imported from managed Tenable Security Center instances. You can manually retrieve scan result data from managed Tenable Security Center instances after the data has been removed from Tenable Security Center Director. The default value is 30 days.

Tip: You can configure vulnerability data expiration for individual asset repositories. For more information, see Asset Repositories.

Mail Settings

The **Mail** option designates SMTP settings for all email-related Tenable Security Center functions. Available options include SMTP host, port, authentication method, encryption, and return address.

In addition, you can use the Test SMTP Settings in the upper left corner of the page to validate the settings.

Option	Description
Test SMTP Settings	Use this button to validate the settings you configure in **SMTP Settings**.
SMTP Settings	
Host	The SMTP server host.
Port	The SMTP server port.
Authentication Method	The authentication method Tenable Security Center Director uses to connect to the SMTP server. Options: **None**, **Login**, **Plain**, **CRAM-SHA1**, **CRAM-MD5**.
Username	The username for authenticating with the SMTP server. **Note:** Type the **Username** in a format supported by your SMTP server (for example, *username@domain.com* or *domain\username*).
Password	The password for authenticating with the SMTP server.
Encryption	The encryption method for the SMTP connection. Options: **None**, **TLS**, **SSL**.
Return Address	The sender email address that appears on outgoing emails from Tenable Security Center Director. **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 server cannot send the email.

Option	Description
Verify Peer	When enabled, Tenable Security Center Director verifies the SMTP server's SSL certificate against trusted certificate authorities.
Verify Peer Name	When enabled, Tenable Security Center Director verifies that the SMTP server's certificate hostname matches the configured **Host** value.
Allow Self Signed Certificates	When enabled, Tenable Security Center Director accepts self-signed SSL certificates from the SMTP server.

Miscellaneous Settings

The **Miscellaneous Configuration** section offers options to configure settings for web proxy, syslog, notifications, and enable or disable some report types.

Web Proxy

> **Note:** These settings are not available in Tenable Enclave Security.

From this configuration page, you can configure a web proxy by entering the host URL (proxy hostname or IP address), port, authentication type, username, and password. The hostname used must resolve properly from the Tenable Security Center Director host.

Syslog

> **Note:** These settings are not available in Tenable Enclave Security.

In the **Syslog** section, you can configure options to allow Tenable Security Center Director to send administrative log events to the local syslog service. For more information about the types of Tenable Security Center Director logs, see the knowledge base article.

Option	Description
Enable Forwarding	Enables administrative log forwarding to the local syslog service.
Facility	The facility that receives the log messages.
Severity	The syslog message levels Tenable Security Center Director forwards: **Informational**, **Warning**, or **Critical**.

Scanning

In the **Scanning** section, you can configure scanning options in Tenable Security Center Director.

Option	Description
IP Randomization	Determines how Tenable Security Center sends active scan target lists to Tenable Nessus and Tenable One Vulnerability Management scanners. This setting enables or disables IP randomization for all configured active scans; you cannot configure IP randomization on a per-scan basis. • When enabled, Tenable Security Center 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. **Scan** / **Randomization** 1,000 or fewer targets / Tenable Security Center randomizes all the IP addresses in the target list.

Option	Description
	<table><tr><th>Scan</th><th>Randomization</th></tr><tr><td>1,001 or more targets</td><td>Tenable Security Center randomizes all the IP addresses in the target list by: - Ordering the IP addresses numerically and splitting them into 100 groups. - Randomly selecting a group and choosing the lowest IP address from that group. - Selecting groups and IP addresses until all IP addresses in all groups are randomized in the target list. </td></tr></table> If the active scan includes a Tenable One Vulnerability Management scanner, Tenable Security Center breaks the target list into smaller lists (256 IP addresses each) before sending to Tenable One Vulnerability Management. **Note:** Some randomized target lists (such as 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 Security Center 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 Security Center sends to each scanner at a time. For more information, see Scan Policy Options.

Notifications

In the **Notifications** section, you can configure options for Tenable Security Center notifications. For more information, see Notifications.

Option	Description
Tenable Security Center Location	The Tenable Security Center web address used when alerts and tickets generate notifications.
Bell Notifications	Enables notifications to appear in the menu in the top navigation bar.

Report Generation

> **Note:** These settings are not available in Tenable Enclave Security.

If your organization requires specialized reporting formats, such as DISA or CyberScope, you can enable **Report Generation** options based on your organization's needs.

- Defense Information Systems Agency (DISA) reporting standards include the Assessment Summary Results (ASR), Assessment Results Format (ARF), and Consolidated Assessment Results Format (CARF) styles.
- CyberScope reports utilize Lightweight Asset Summary Results Schema (LASR) style reports, which are used by some segments of governments and industry.

To allow users to choose these reports during report creation, you must enable the corresponding toggles. For more information about reports in Tenable Security Center, see Reports.

Option	Description
Enable DISA ARF	Enable the DISA ARF report format, which meets the standards of the Defense Information Systems Agency Assessment Results Format.
Enable DISA	Enable the DISA consolidated ARF report format, which meets the

Option	Description
Consolidated ARF	standards of the Defense Information Systems Agency Consolidated Assessment Results Format.
Enable DISA ASR	Enable the DISA ASR report format, which meets the standards of the Defense Information Systems Agency Assessment Summary Results.
Enable CyberScope	Enable the CyberScope report format, which meets CyberScope reporting standards to support FISMA compliance.

PostgreSQL Connection

If you have configured an external PostgreSQL database, this section displays the connection information for the database. For more information about PostgreSQL with Tenable Security Center Director, see External PostgreSQL with Tenable Security Center Director.

Privacy

The **Enable Usage Statistics** option specifies whether Tenable collects anonymous telemetry data about your Tenable Security Center 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 Security Center license, and your configured features. Tenable uses the data to improve your user experience in future Tenable Security Center 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 Security Center users must refresh their browser window for the changes to take effect.

License Settings

Note: These settings are not available in Tenable Enclave Security.

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

For information about the Tenable Security Center 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 Security Center and the feed and plugin update (scanner update) schedules.

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

Update	Description
Tenable Security Center Feed	Retrieves the latest Tenable Security Center feed from Tenable. This feed includes data for general use, including templates (for example, dashboards, ARCs, reports, policies, assets, and audit files), template-required objects, some general plugin information, and updated VPR values.
Active Plugins	Retrieves the latest active plugins feed (for Tenable Nessus and Tenable One Vulnerability Management scanners) from Tenable. Tenable Security Center pushes the feed to Tenable Nessus and Tenable One Vulnerability Management scanners.
Passive Plugins	Retrieves the latest passive plugins feed from Tenable. Tenable Security Center pushes the feed to Tenable Network Monitor instances.
WAS Plugins	Retrieves the latest Tenable One Web App Scanning plugins feed from Tenable. Tenable Security Center Director pushes the feed to Tenable One Web App Scanning instances.

For information about Tenable Security Center-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 appear.

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

> **Note:** Tenable Security Center cannot translate text within custom files. Upload a translated **Active Plugins.xml** file to display the file content in a local language.

For more information, see Configure Plugin Text Translation.

Schedules

Tenable Security Center automatically updates Tenable Security Center 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.

Security Center Software Updates

The **Security Center Software Updates** section includes options for applying updates and patches for Tenable Security Center.

In the **Authorization Token** box, enter your authorization token. You can generate an authorization token on the Tenable Downloads API page.

If you enable the **Automatically Update Through the Security Center Feed** option, then Tenable Security Center automatically applies any available Tenable Security Center patches during scheduled feed updates.

Note: Some patches cannot be applied through the feed, and must be installed manually.

Available Software Updates

New updates and patches for Tenable Security Center appear in the **Available Software Updates** section of the **Plugins/Feed Configuration** page.

The **Install Now** tab displays available software updates for download. You can install them immediately by selecting the check box and clicking **Install Now**. If you enable the **Automatically Update Through the Security Center Feed** option in the **Security Center Software Updates** section, then Tenable Security Center will automatically apply these updates and patches during scheduled feed updates.

The **Install Manually** tab includes software updates that must be installed manually. You can download the files for these updates and patches from the Tenable Downloads page.

If you install a software update but the installation fails, the update will appear in the **Available Software Updates** section with a warning icon. Click the software update in the table to view details about the error.

Installed Software Updates

When you install a software update, it moves from the **Available Software Updates** section to the **Installed Software Updates** section. If a software update requires a restart to finish installing, the status for the update in the **Installed Software Updates** section will be **Needs Restart**. After you complete a software update, the status for the update will be **Installed**.

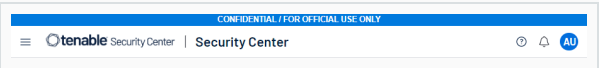
SAML Settings

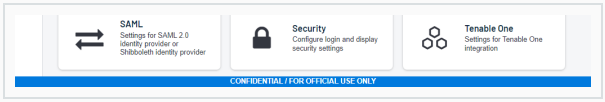
Use the SAML section to configure SAML 2.0-based SAML authentication (for example, Okta, OneLogin, Shibboleth 2.0, etc.) for Tenable Security Center users. For more information, see SAML Authentication.

Security Settings

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

Option	Description
Authentication Settings	
Session Timeout	The web session timeout in minutes. The default is *60*.
Maximum Login Attempts	The number of failed login attempts allowed before Tenable Security Center locks the account. The default is *20*. To disable this feature, set the value to *0*.
Minimum Password Length	The minimum number of characters for passwords using local TNS authentication. For new installations, the default and minimum value is *12*, and Tenable Security Center enforces this length whether or not **Password Complexity** is enabled. **Note:** If you upgrade to Tenable Security Center 6.10 or later, Tenable Security Center retains your existing password settings. If you later change the password settings, you cannot set the **Minimum Password Length** below *12*. Changing the setting does not affect existing passwords; the new length applies the next time a user changes their password.
Password Complexity	Requires passwords to contain the following. This option is enabled by default for new installations: • At least one uppercase letter • At least one lowercase letter • At least one numerical character • At least one special character

Option	Description
	Note: After you enable **Password Complexity**, Tenable Security Center prompts all users to reset their passwords the next time they log in to Tenable Security Center.
Startup Banner Text	Type the text banner that appears before to the login interface.
User Text	Adds custom text to the bottom of the user profile menu. You can use the text to identify a company, group, or other organizational information (maximum 128 characters).
Classification Type	Adds a header and footer banner to Tenable Security Center to indicate the classification of the data accessible via the software. Current options are **None**, **Custom, Unclassified**, **Confidential**, **Secret**, **Top Secret**, and **Top Secret - No Foreign**. If you select **Custom**, the following options appear: • **Custom Text** - Type the text that you want to appear in the banner (maximum 128 characters). • **Text Color** - Select the text color for the banner. • **Background Color** - Select the background color for the banner. **Note:** Custom banners in reports are supported only for Arial Regular font. Sample header:  Sample footer:

Option	Description
	 **Note:** If you set **Classification Type** to an option other than **None**, users can only see the plain report styles. The Tenable report styles do not support the classification banners.
Allow API Keys	When enabled, allows users to generate API keys as an authentication method for Tenable Security Center API requests. For more information, see Enable API Key Authentication.
Allow Session Management	This setting is disabled by default. When enabled, the **Session Limit** option appears. This feature displays the option that allows administrators to set a session limit for all users.
Disable Inactive Users	When enabled, Tenable Security Center disables user accounts after a set period of inactivity. You cannot use a disabled user account to log in to Tenable Security Center, but other users can use and manage objects owned by the disabled user account.
Days Users Remain Enabled	When you enable **Disable Inactive Users**, specify the number of inactive days you want to allow before automatically disabling a user account.
Session Limit	Specifies the maximum number of sessions a user can have open at once. If you log in and the session limit has already been reached, Tenable Security Center notifies you 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. **Note:** This behavior is different for Common Access Cards (CAC) logins.

Option	Description
	Tenable Security Center does not check active sessions for CAC authentication.
Login Notifications	Sends notifications for each time a user logs in.
WebSeal	Allows you to enable or disable WebSEAL. WebSEAL supports multiple authentication methods, provides Security Access Authorization service, and single sign-on capabilities. **Caution:** Before the user that enabled WebSEAL logs out of Tenable Security Center, Tenable Security Center strongly recommends confirming, in a separate session, that at least one user (preferably an administrator user) is able to log in successfully via WebSEAL. Otherwise, if there is an issue, no one will be able to access Tenable Security Center to turn off WebSEAL. **Caution:** Any user created while WebSEAL is enabled will not have a password. An administrator must update the user account to establish a password. Any user that existed before enabling WebSEAL must revert to their old password.
PHP Serialization	
Operational Status	Summarizes your current setting.
PHP Serialization Mode	Specifies whether you want to allow or prevent PHP serialization in Tenable Security Center. • **PHP Serialization ON** – Tenable Security Center performs PHP serialization and Tenable Security Center features operate as expected.

Option	Description

	• **PHP Serialization OFF** – Tenable Security Center does not perform PHP serialization and prevents users from importing or exporting the following objects:
	  • Assets
	  • Scan policies
	  • Assurance Report Cards
	  • Reports
	  • Audit files
	  • Dashboards

FIPS 140-2 Configuration	
Operational Status	Summarizes whether FIPS 140-2 mode is currently enabled or disabled.
FIPS 140-2 Mode	Specifies whether you want to enable or disable FIPS mode for communication. Switching from one mode to the other requires a restart. For more information, see Start, Stop, or Restart Tenable Security Center Director.

Edit Plugin and Feed Settings and Schedules

Required Tenable Security Center 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 Security Center Director via the user interface.
2. In the left navigation, click **System** > **Configuration**.

The **Configuration** page appears.

3. Click the **Plugins/Feed** tile.

   The **Plugins/Feed Configuration** page appears.

4. View the **Plugin Detail Locale** section to see the local language configured for Tenable Security Center Director.

5. Expand the **Schedules** section to show the settings for the **Tenable Security Center Feed**, **Active Plugins**, **Passive Plugins**, or **Event Plugins** schedule.

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

      - If there is an update available, the **Update** link will be active.
      - If your plugins or feed are already up to date, the **Update** link will be inactive.

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

   c. Click **Submit**.

      Tenable Security Center Director saves your configuration.

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

1. Log in to Tenable Security Center Director via the user interface.
2. In the top navigation bar, click your user profile (SC) icon > **Feeds**.

   The **Plugins/Feed Configuration** page appears.

3. View the **Plugin Detail Locale** section to see the local language configured for Tenable Security Center Director.

4. Expand the **Schedules** section to show the settings for the **Tenable Security Center 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 Security Center Director saves your configuration.

Configure Plugin Text Translation

Required Tenable Security Center User Role: Administrator

For more information, see Configuration Settings.

To configure plugin text translation:

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, click **System** > **Configuration**.

   The **Configuration** page appears.
3. Click the **Plugins/Feed** tile.

   The **Plugins/Feed Configuration** page appears.
4. If you want plugin text to display in a local language, select a language from the **Locale List** box.
5. Click **Apply**.

   Tenable Security Center Director saves your configuration.
6. In the **Schedules** section, in the **Active Plugins** row, click **Update**.

   Tenable Security Center updates active plugins 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 Security Center API requests. Without API keys, users must use the `/token` endpoint to log in to the Tenable Security Center API and establish a token for subsequent requests, as described in Token in the *Tenable Security Center API Guide*.

Tenable Security Center 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 can 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 can use API keys for Tenable Security Center API request authentication by including the **x-apikey** header element in your HTTP request messages, as described in API Key Authorization in the *Tenable Security Center API Best Practices Guide*.

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

For more information about the Tenable Security Center API, see the *Tenable Security Center API Guide* and the *Tenable Security Center API Best Practices Guide*.

Manage API Key Authentication

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

Enable API Key Authentication

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

To allow users to authenticate to the Tenable Security Center API using API keys:

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, 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 Security Center Director saves your configuration.

What to do next:

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

Disable API Key Authentication

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 Security Center reauthorizes any API keys they were active before you disabled API key authentication.

To disable API key authentication:

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, 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 Security Center Director saves your configuration.

Diagnostics Settings

This page displays and creates information that assists in troubleshooting issues that may arise while using Tenable Security Center Director.

System Status

You can use this section to view the current status of system functions.

System Function	Description
Correct Java Version	Indicates whether the minimum version of Java required to support Tenable Security Center Director functionality is installed. For more information, see Before You Upgrade.
Sufficient Disk Space	Indicates whether you have enough disk space to support Tenable Security Center Director functionality. A red X indicates the disk is at 95% capacity or higher. For more information, see Hardware Requirements.
Correct RPM Package Installed	Indicates whether you have the correct Tenable Security Center Director RPM installed for your operating system. For more information, see System Requirements.
Debugging	Indicates whether debugging is enabled. You may experience performance and storage issues if you leave debugging enabled for extended periods of time. For more information, see Debugging Logs.
Migration Errors	Indicates whether an error occurred during a recent Tenable Security Center Director update.
PHP Integrity Errors	Indicates whether any PHP files have been modified from the original version included in the Tenable Security Center Director RPM.
PostgreSQL Connection Errors	Indicates whether any database connection errors have occurred.

Diagnostics File

You can use this section to generate a diagnostics file for troubleshooting with Tenable Support. You can download the file to share with Tenable Support manually, or you can send the file directly to an existing Tenable Support case. For more information, see Generate a Diagnostics File.

Debugging Logs

You can use this section to enable or disable debugging logs for troubleshooting with Tenable Support. For more information, see Manage Debugging Logs.

> **Caution:** Debugging logs can fill your disk and disrupt system processes if left enabled. Only enable debugging logs when instructed by Tenable Support, and disable them immediately after troubleshooting is complete.

Generate a Diagnostics File

> **Required Tenable Security Center User Role:** Administrator

Tenable Support may ask you to generate a diagnostics file to assist with troubleshooting. The `debug.zip` diagnostics file contains files related to the selected chapters. For more information about diagnostics file options, see Diagnostics File Options.

You can generate a diagnostics file in one of two ways:

- **Create Diagnostics File** – Tenable Security Center Director generates the diagnostics file and you download it, then share it with Tenable Support.
- **Create & Send to Support** – Tenable Security Center Director generates the diagnostics file, uploads it to the Tenable file-uploads portal, and links it to an existing Tenable Support case that you select.

For more information about Tenable Security Center diagnostics, see Diagnostics Settings.

To generate a diagnostics file for Tenable Support:

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, 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**.

   Tenable Security Center Director generates the diagnostics file.

7. Click **Download Diagnostics File**.

   The `debug.zip` file downloads.

To create a diagnostics file and send it to a Tenable Support case:

> **Note:** Tenable Security Center must be able to resolve and reach *https://file-uploads.tenable.com* with a valid Tenable Nessus feed subscription.

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, click **System** > **Diagnostics**.

   The **Diagnostics** page appears.

3. In the **Diagnostics File** section, in the **Support Case** drop-down, select the support case you want to link the diagnostics file to.

4. Click **Create Diagnostics File & Send to Support**.

   The page updates with options to configure the diagnostics file.

5. In the **General** section, if you want to omit IP addresses from the diagnostics file, click to enable the **Strip IPs from Chapters** toggle.

6. In the **Chapters** section, click the toggles to enable or disable the chapters you want to include in the diagnostics file.

7. Click **Create Diagnostics File & Send to Support**.

Tenable Security Center Director generates the diagnostics file, uploads it to the Tenable file-uploads portal, and links it to the support case you selected.

What to do next:

- Share the `debug.zip` file with Tenable Support for troubleshooting.

Diagnostics File Options

For more information, see Diagnostics Settings and Generate a Diagnostics File.

Option	Description	Default
General		
Strip IPs from Chapters	When enabled, Tenable Security Center omits IP addresses from the following files: • `sc-configuration.txt` • `sc-scans.txt` • `sc-setup.txt` • `sc-logs.txt` • `sc-error.log` • `cert.log` • `install.log` • `upgrade.log` • `schemaUpdates*.log` • `sc-environment.txt` • `sc-telemetry.txt` • `/opt/sc/support/error_Log` • `/opt/sc/support/*.conf`	Disabled

Option	Description	Default
Chapters		
System Information	Include information about the Tenable Security Center host system in the diagnostic file (`sc-systeminfo.txt`).	Enabled
Scan Information	Include information about scans, scan results, and freeze windows in the diagnostic file (`sc-scaninfo.txt`). For more information, see Active Scans, Agent Scanning, and Freeze Windows.	Enabled
Setup	Include information about the following Tenable Security Center resources in the diagnostic file (`sc-setup.txt`): • Active users • Tenable Nessus Scanners • Tenable Network Monitor Instances • Scan Zones • Schedules • Job Queue Events • Asset Tags • Repositories • Organizations • User Roles • Reports • Report results • Audit Files	Enabled

Option	Description	Default
Logs	Include administrator logs, organization logs, Tenable Security Center error logs, and the certificate log in the diagnostic file (`sc-logs.txt`, `sc-error.log`, and `cert.log`).	Enabled
Environment	Include information about the `tns` user environment in the diagnostic file (`sc-environment.txt`).	Enabled
Directory Listing	Include a directory listing in the diagnostic file (`sc-dirlisting.txt`). For more information, see Tenable Security Center Communications and Directories.	Enabled
Dependency	Include information about Tenable Security Center dependencies in the diagnostic file (`sc-depsinfo.txt`). For more information, see Dependencies.	Enabled
Upgrade Log	Include a log of Tenable Security Center upgrade events in the diagnostic file (`upgrade.log`).	Enabled
Install Log	Include a log of Tenable Security Center installation events in the diagnostic file (`install.log`).	Enabled
Apache Log	Include a log of web server requests in the diagnostic file (`/opt/sc/support/error_Log`).	Enabled
PostgreSQL Log	Include the PostgreSQL database server log file in the diagnostic file (`postgresql.log`) .	Enabled
PostgreSQL	Include PostgreSQL configuration details and status	Enabled

Option	Description	Default
Debug	information in the diagnostic file (`sc-postgres-details.txt`).	
Application Conf	Include Tenable Security Center configuration details in the diagnostic file (`sc-configuration.txt`).	Enabled
Server Conf	Include server configuration details in the diagnostic file (`/opt/sc/support/*.conf`).	Enabled
User Information	Include a list of users in the diagnostic file (`sc-users.txt`). The list includes the following details: • For administrators, the user ID and role ID • For organizational users, the user ID, role ID, and group ID For more information about ID values, see View User Account Details, View User Role Details, and View Group Details.	Enabled
Include Names	(If **User Information** is enabled) Include usernames and user display names for each user in the diagnostic file. For more information, see User Account Options. **Tip**: The display name combine's the user's **First Name** and **Last Name**.	Disabled
Director Information	Include details about your Tenable Security Center Director license and managed Tenable Security Center instances in the diagnostic file (`sc-director.txt`).	Enabled

Manage Debugging Logs

Required Tenable Security Center User Role: Administrator

For more information about debugging logs, see Debugging Logs.

Caution: Debugging logs can fill your disk and disrupt system processes if left enabled. Only enable debugging logs when instructed by Tenable Support, and disable them immediately after troubleshooting is complete.

Note: Collected debug logs contained in the debug archive are automatically deleted during the scheduled nightly cleanup.

Enable Debugging Logs

You can enable debugging to generate logs for troubleshooting with Tenable Support.

Caution: Tenable does not recommend enabling debugging logs unless instructed by Tenable Support. Some debugging settings generate large volumes of data that can fill your disk if left enabled. Others may affect system processes beyond logging. Disable all debugging settings as soon as troubleshooting is complete.

To enable debugging:

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, click **System** > **Diagnostics**.

   The **Diagnostics** page appears.
3. In the **Debugging Logs** section, select one or more debugging logs Tenable Support asked you to enable.
4. Click **Save Debug Settings**.

   Tenable Security Center Director enables the debugging logs you selected and saves the corresponding log files to `/opt/sc/admin/logs`.

What to do next:

- Download the debugging logs, as described in Download Debugging Logs.
- Share the debugging log files with Tenable Support.
- Disable all debugging logs as soon as troubleshooting is complete, as described in Disable Debugging Logs. Leaving debugging logs enabled can fill your disk and affect system performance.

Download Debugging Logs

You can download debugging logs for troubleshooting with Tenable Support.

Before you begin:

- Enable debugging logs, as described in Enable Debugging Logs.

To download debugging logs:

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, click **System** > **Diagnostics**.

   The **Diagnostics** page appears.
3. In the **Download Debugging Logs** section, click **Collect Log Files**.

   Tenable Security Center generates the debugging log files you selected.
4. Click **Download Debug File**.

   The debugging logs download.

What to do next:

- Share the files with Tenable Support.
- Disable all debugging logs as soon as troubleshooting is complete, as described in Disable Debugging Logs. Leaving debugging logs enabled can fill your disk and affect system performance.

Disable Debugging Logs

To disable debugging:

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, click **System** > **Diagnostics**.

   The **Diagnostics** page appears.
3. In the **Debugging Logs** section:
   - To disable individual debugging logs, deselect the logs.
   - To disable all debugging logs, click **Deselect All**.
4. Click **Save Debug Settings**.

   Tenable Security Center Director disables the debugging logs you deselected.

What to do next:

- Follow Tenable Support's instructions to manually remove old debugging log files from `/opt/sc/admin/logs`.

Job Queue Events

Path: **System** > **Job Queue**

Job Queue is a Tenable Security Center 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 Security Center Director processes.

System Logs

Tenable Security Center Director logs contain detailed information about functionality to help you 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 Security Center Director or perform basic

functions. For example, you can track when users change passwords. Administrators in Tenable Security Center Director can view system logs for managed Tenable Security Center instances.

To view system logs:

1. Log in to Tenable Security Center Director via the user interface.
2. Depending on your user role, perform one of the following actions:
    - **Administrator users:** In the left navigation, click **System** > **System Logs**.
    - **Organizational users:** In the top navigation, click your username > **System Logs**.

    The **System Logs** page appears.
3. (Optional) 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.

Option	Description
Name	Type a name for the publishing site.
Description	Type a description of the publishing site.
Type	The method Tenable Security Center 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.
Max Chunk Size (MB)	If the target is a CMRS site, Tenable sends the report in chunks sized according to this value.

Option	Description
URI	The target address to send the report to when completed.
Use Proxy	When enabled, the publishing site leverages the web proxy defined in the Web Proxy settings.
Authentication	There are two methods of authentication available: **SSL Certificate** and **Password**.
Username / Password	If you select **Password** as the **Authentication** method, the credentials to authenticate to the target publishing server.
Certificate	If you selected **SSL Certificate** as the **Authentication** method, the certificate you want to use for authentication.
Organizations	Select the organization(s) that are allowed to publish to the configured site.
Verify Host	When enabled, Tenable Security Center Director verifies that the target address specified in the **URI** option matches the CommonName (CN) in the SSL certificate from the target publishing server.

Keys Settings

Keys allow administrator users to use key-based authentication with a remote Tenable Security Center. This also removes the need for Tenable Security Center administrators to know the administrator login or password of the remote system.

Tenable Security Center Director uses ED25519 keys to authenticate to other Tenable Security Center Director instances.

Note: The ED25519 public key from the local Tenable Security Center must be added to the **Keys** section of the Tenable Security Center 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 information about adding, downloading, and deleting keys, see Manage Keys.

Note: Tenable Security Center Director only supports keys that are FIPS-140-2 compliant:

- RSA: Supported for key lengths from 1024 to 16384 bits, often used for signature verification and key encryption.
- DSA: Supported for signature verification, with common lengths being 2048 or 3072 bits.
- EC DH: Supported for public key agreement on all NIST-defined P curves.

Manage Keys

Required Tenable Security Center User Role: Administrator

For more information about ED25519 keys in Tenable Security Center Director, see Keys Settings.

Add a Key

To add a new key:

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, click **System** > **Keys**.

   The **Keys** page appears.
3. At the top of the table, click **Add**.

   The **Add Key** page appears.
4. In the **Type** drop-down, select **DSA**, **RSA**, or **ED25519**.
5. In the **Comment** 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 Security Center.
7. Click **Submit**.

   Tenable Security Center Director saves your configuration.

Download the Tenable Security Center Director SSH Key

You can download the Tenable Security Center Director ED25519 key on the **Keys** page.

> **Note:** Tenable Security Center Director authenticates to Tenable Security Center Director with ED25519 keys. If your Tenable Security Center Director remote repository still uses an RSA or ECDSA key, it will continue to use the RSA or ECDSA key until you add the ED25519 key to the remote repository.

To download the Tenable Security Center Director SSH key:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **System** > **Keys**.
3. At the top of the table, click **Download Tenable Security Center Key**.

   The Tenable Security Center Director ED25519 key downloads.

Delete a Key

To delete a key:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **System** > **Keys**.
3. Select the key you want to delete:
   - To delete a single key:
     a. In the table, right-click the row for the key you want to delete.

        The actions menu appears.

     b. Click **Delete**.
   - To delete multiple keys:
     a. In the table, select the check box for each key you want to delete.

        The available actions appear at the top of the table.

     b. At the top of the table, click **Delete**.

A confirmation window appears.

4. Click **Delete**.

   Tenable Security Center deletes the key.

User Profile Menu Settings

The user profile SC icon in the top navigation bar opens a menu with options to manage your user account.

> **Note:** Depending on the screen resolution, the username may not appear next to the user icon in the top navigation bar.

About

Path: Your user profile SC icon > **About**

The **About** menu item displays the Tenable Security Center Director version, Server Build ID, and copyright information.

System Logs (Organizational Users Only)

Path: Your user profile SC icon > **System Logs**

For a complete discussion about system logs, see System Logs.

Profile (Organizational Users Only)

Path: Your user profile SC icon > **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 Account Options.

Feeds (Organizational Users Only)

Path: Your user profile SC icon > **Feeds**

The **Feeds** option displays information about the Tenable Security Center Director feeds and plugin sets and, if permitted, a link to update the plugins either through Tenable Security Center Director or by manually uploading plugins. The displayed feeds are for Tenable Security Center Feed, Active Plugins, Passive Plugins, and Event Plugins. You can only update feeds with valid Activation Codes.

Plugins are scripts used by the Tenable Nessus and Tenable Network Monitor servers to interpret vulnerability data. For ease of operation, Tenable Security Center Director centrally manages Tenable Nessus and Tenable Network Monitor plugins and pushes the plugins out to their respective scanners.

For more information about plugin/feed settings, see Configuration Settings and Edit Plugin and Feed Settings and Schedules.

Notifications

Path: Your user profile SC icon > **Notifications** *or* 🔔 icon > **Show More**

In Tenable Security Center, specified events can display a pop-up in the lower right-hand corner of the Tenable Security Center user interface.

Some events in Tenable Security Center Director will cause a notification to appear in the 🔔 icon in the top navigation bar.

For more information, see Notifications.

Plugins

Path: Your user profile SC icon > **Plugins**

Plugins are scripts used by the Tenable Nessus and Tenable Network Monitor servers to interpret vulnerability data. For ease of operation, Tenable Nessus and Tenable Network Monitor plugins are managed centrally by Tenable Security Center and pushed out to their respective scanners.

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: Your user profile SC icon > **Help**

The **Help** option opens the *Tenable Security Center Director User Guide* section for your page. To access other Tenable documentation, see docs.tenable.com.

Logout

To end your session in Tenable Security Center Director, click your user profile SC icon > **Logout**.

Tenable recommends closing your browser window after logging out.

Custom Plugin Packages for NASL and CA Certificate Upload

> **Note:** Tenable does not support troubleshooting custom plugin packages for NASL.

> **Note:** Linked Tenable Nessus scanners do not support custom plugins. Custom plugins are only supported on active (managed) scanners. For more information, see Linked Scanning Overview.

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 Security Center 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 Tenable Nessus scanning issue.

After you Manage Custom Plugin Packages, Tenable Security Center Director pushes the package to Tenable 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 Security Center Director or Tenable Nessus. The exception is the `custom_CA.inc` file, which the system merges with the existing CA certificates. For more information, see custom_CA.inc Guidelines.

`custom_feed_info.inc` Guidelines

Always include this file to time stamp your upload to Tenable Security Center Director. This text file must contain the following lines:

```
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 Security Center 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 Security Center 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 Tenable 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
-----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
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
certificate2text
certificate2text
certificate2text
certificate2text
-----END CERTIFICATE-----
```

How Uploads Affect Existing CA Certificates

When you upload a custom plugin package that includes a `custom_CA.inc` file, Tenable Security Center Director adds the CA certificates in the uploaded file to the CA certificates that are already

stored. The upload does not replace the existing certificates. For example, if you previously uploaded three certificates and then upload a package that contains two new certificates, Tenable Security Center Director stores all five.

- If a certificate appears in both the existing and the uploaded file, Tenable Security Center Director stores it only once. Tenable Security Center Director recognizes duplicate certificates even if their line endings or whitespace differ.
- The order of the certificates in the file does not matter.
- If you have not uploaded a `custom_CA.inc` file before, Tenable Security Center Director uses the uploaded file as is.
- Tenable Security Center Director applies the merge only if the upload succeeds. If a custom plugin in the package fails validation, Tenable Security Center Director does not apply the package and keeps your existing CA certificates.

Tenable Security Center Director records each merge in the administrator log. For example: `Merged CA bundle: 3 existing + 2 new = 5 total certificates`.

Reset the CA Certificate Bundle

To remove all previously stored CA certificates and replace them with only the certificates in your new `custom_CA.inc` file, include an empty `.sc_reset_ca` file in your custom plugin package.

To reset the CA certificate bundle:

1. In the command line interface (CLI), create an empty file named `.sc_reset_ca`:

   ```
   # touch .sc_reset_ca
   ```

2. Prepare a new `custom_CA.inc` file that contains only the CA certificates you want to keep.
3. Tar and compress the files together, including `.sc_reset_ca` in the root of the package. For example:

   ```
   # tar -zcvf upload_this.tar.gz custom_feed_info.inc custom_CA.inc .sc_reset_ca
   ```

4. Upload the package, as described in Upload the Custom Plugin Package.

   Tenable Security Center Director skips the merge, replaces the stored CA certificates with the certificates in the uploaded `custom_CA.inc` file, and removes the `.sc_reset_ca` file. Tenable Security Center Director records the reset in the administrator log: `Custom CA bundle reset - replaced with new bundle`.

Note: A reset removes every CA certificate that you uploaded previously. Include all the certificates that you still need in the new `custom_CA.inc` file.

Manage Custom Plugin Packages

Required Tenable Security Center User Role: Administrator or Security Manager

You can upload a custom plugin package as a `.tar.gz` or `.tgz` file. For more information about custom plugin packages, see Custom Plugin Packages for NASL and CA Certificate Upload.

Create the Custom Plugin Package

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.

   Note: After upload, the system untars the files within your custom plugin package and overwrites any identically named files already in Tenable Security Center Director or Tenable Nessus. The exception is the `custom_CA.inc` file, which Tenable Security Center Director merges with the CA certificates that are already stored. For more information, see How Uploads Affect Existing CA Certificates.

2. In the command line interface (CLI), 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.

Upload the Custom Plugin Package

Upload the `.tar.gz` or `.tgz` file to Tenable Security Center Director:

1. Log in to Tenable Security Center 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 that you created in Create the Custom Plugin Package.
4. Click **Submit**.

   Tenable Security Center Director uploads the package and pushes it to Tenable 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 Tenable Nessus has the custom plugin bundle by checking its plugin directory.

Backup and Restore

Tenable recommends performing regular backups of the Tenable Security Center Director data in your `/opt/sc` directory. When you restore a backup, the file overwrites the content in your `/opt/sc` directory.

Data backup requirements:

- You must restore a backup file to a Tenable Security Center Director running the same version. For example, you cannot restore a backup file created on version 6.0.0 to a Tenable Security Center Director running Tenable Security Center 6.1.0.
- You must restore a backup file to a Tenable Security Center Director host with the same hostname as the host where the backup was created. For example, you cannot restore a backup file created on a Tenable Security Center Director with the hostname *Example1* to a Tenable Security Center Director with the hostname *Example2*.

For more information, see Perform a Backup and Restore a Backup.

Configuration Backups

Tenable recommends performing regular backups of your Tenable Security Center Director configuration and managed Tenable Security Center instance configurations in addition to your Tenable Security Center Director data. You can restore a configuration backup to quickly resume normal Tenable Security Center Director operation as part of your disaster recovery plan.

Tenable Security Center Director configuration backups do not include configurations for managed Tenable Security Center instances, such as scans, scan policies, or credentials. You must perform a separate backup for each Tenable Security Center instance.

Configuration backups do not include data (such as vulnerability data, trend data, licenses, or secure connection settings). When your repositories contain new vulnerability data, you can use your dashboards, reports, and analysis tools to assess your network.

> **Note:** After you restore a configuration backup, Tenable recommends performing discovery scans to re-populate your repositories with vulnerability data. For more information, see Scanning Overview.

Configuration backup requirements

You must restore a backup file to a Tenable Security Center Director running the same version. For example, you cannot restore a backup file created on version 6.2.0 to a Tenable Security Center Director running Tenable Security Center 6.2.1.

Note: For best performance, after restoring a configuration backup, ensure the hostname associated with the configuration backup file matches the hostname on the receiving Tenable Security Center Director.

For more information, see Perform a Configuration Backup and Restore a Configuration Backup.

Configurations Included in a Configuration Backup

Category	Configurations
Users	User accounts, user roles, groups, and organizations
Resources	Managed Tenable Security Center instances, LDAP servers
System	Configuration settings (including data expiration settings, mail settings, miscellaneous settings, license settings, plugins/feed settings, SAML settings, and security settings), publishing sites settings, keys settings, and schedules
Scanning	Audit files, asset tags, and repositories
Reporting	Dashboards, report definitions, report images, and CyberScope and DISA report attributes
Workflow	Alerts
Analysis	Queries

Note: In Tenable Security Center Director 6.10 and later, configuration backups include Nessus scanner and scan zone data, but not scanner credentials. After you restore a configuration backup, re-enter the credentials for each Nessus scanner. Configuration backups also do not include trending data (other than trending configuration) or license keys. For more information, see Restore a Configuration Backup.

Automatic Backups

Tenable Security Center Director performs automatic nightly backups of the following databases:

- `/opt/sc/application.db`
- `/opt/sc/hosts.db`
- `/opt/sc/jobqueue.db`
- `/opt/sc/plugins.db`
- `/opt/sc/remediationHierarchy.db`
- `/opt/sc/orgs/<orgID>/organization.db` (for each organization in your Tenable Security Center Director)
- `/opt/sc/orgs/<orgID>/assets.db` (for each organization in your Tenable Security Center Director)

Automatic backups run nightly at 1:20 AM local time. This schedule cannot be changed.

Tenable Security Center Director stores backups in the same directory as the database.

Perform a Backup

> **Required Tenable Security Center User Role:** Root user

For more information about the backup and restore process, see Backup and Restore.

To perform a backup of Tenable Security Center Director data:

1. Log in to Tenable Security Center Director via the command line interface (CLI).
2. Stop Tenable Security Center Director with the following command:

   ```
   # /bin/systemctl stop SecurityCenter
   ```

   Tenable Security Center Director stops.
3. In the CLI in Tenable Security Center Director, 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 (including scans) running on Tenable Security Center Director.

5. If necessary, repeat step 4 to confirm all processes stopped.
6. If you have configured an external PostgreSQL database, back up the database using `pg_dump` or a similar utility. Save the database backup file in a secure location.
7. Run the following command to create a `.tar` file for your `/opt/sc` directory:

```
# tar -pzcf sc_backup.tar.gz /opt/sc
```

> **Note:** The `.tar` file switches are case-sensitive.

Tenable Security Center Director creates the backup file.

8. Run the following command to confirm the backup file is not corrupted:

```
# tar -tvf sc_backup.tar.gz
```

9. Move the backup file to a secure location.
10. Start Tenable Security Center Director with the following command:

```
# /bin/systemctl start SecurityCenter
```

Tenable Security Center Director starts.

What to do next:

- (Optional) Restore the backup file, as described in Restore a Backup.

Restore a Backup

Required Tenable Security Center 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 Security Center Director, as described in Perform a Backup.
- Confirm your receiving Tenable Security Center Director meets the requirements described in Backup and Restore.
- Move the backup file to your receiving Tenable Security Center Director's `/tmp` directory.

To restore a backup file:

1. Log in to Tenable Security Center Director via the command line interface (CLI).
2. Stop Tenable Security Center Director, as described in Start, Stop, or Restart Tenable Security Center Director.

   Tenable Security Center Director stops.
3. In the CLI in Tenable Security Center Director, 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 Security Center Director.
5. If necessary, repeat step 4 to confirm all processes are stopped.

6. Empty the `/opt/sc` folder of all contents by running the following commands:

```
# cd /opt/
```

```
# rm -rf sc/
```

7. If you have configured an external PostgreSQL database, restore the database from the backup file you created in Perform a Backup.
8. Run the following commands to decompress the `.tar` file:

```
# cd /
```

```
# tar -xvf /tmp/sc_backup.tar.gz
```

> **Note:** The `.tar` file switches are case-sensitive.

The restore finishes.

9. Start Tenable Security Center Director, as described in Start, Stop, or Restart Tenable Security Center Director.

Tenable Security Center Director starts.

Perform a Configuration Backup

> **Required Tenable Security Center User Role:** Root user

For more information about the backup and restore process and the configurations included in a configuration backup, see Backup and Restore.

Before you begin:

- If you uploaded custom plugins, save a copy of your custom plugins in a safe location.

To perform a backup of your Tenable Security Center Director configuration:

1. Log in to Tenable Security Center Director via the command line interface (CLI).
2. Stop Tenable Security Center Director with the following command:

   ```
   # /bin/systemctl stop SecurityCenter
   ```

   Tenable Security Center Director stops.
3. Start the PostgreSQL database with the following command. The configuration backup includes Tenable Security Center Director data stored in PostgreSQL, so the database must be running when you perform the backup.

   ```
   su - tns -c "/opt/sc/support/bin/pg_ctl start -D /opt/sc/data/postgresql/"
   ```

   Note: If you use an external PostgreSQL database, ensure the database is running and skip this step.
4. In the CLI in Tenable Security Center Director, do one of the following:
   - To save the configuration backup file to a local directory, run the following command, where [*local directory path*] is the local directory where you want to save the backup file:

     ```
     /opt/sc/support/bin/php /opt/sc/src/tools/backupSCConfiguration.php -l [local directory path]
     ```

     For example:

     ```
     /opt/sc/support/bin/php /opt/sc/src/tools/backupSCConfiguration.php -l /tmp/
     ```
   - To save the configuration backup file to a remote directory, run the following command, where [*remote directory absolute path*] is the absolute path to the remote directory where you want to save the backup file:

```
/opt/sc/support/bin/php /opt/sc/src/tools/backupSCConfiguration.php -r [user]@[host]:[remote absolute path to configuration backups directory]
```

For example:

```
/opt/sc/support/bin/php /opt/sc/src/tools/backupSCConfiguration.php -r tns@100.100.100.100:/tmp/
```

Tenable Security Center creates the configuration backup file and saves it to the specified directory.

Tip: The configuration backup file name includes the backup date and time, the Tenable Security Center hostname, and the Tenable Security Center version (for example, `SC-config-20211101-165111-sc-hostname-5_20_0.tar.gz`).

5. Stop the PostgreSQL database with the following command:

```
su - tns -c "/opt/sc/support/bin/pg_ctl stop -D /opt/sc/data/postgresql/ -m fast"
```

Note: If you use an external PostgreSQL database, skip this step.

6. Start Tenable Security Center Director with the following command:

```
# /bin/systemctl start SecurityCenter
```

Tenable Security Center Director starts.

What to do next:

- Perform a backup for your managed Tenable Security Center instances, as described in Perform a Configuration Backup in the *Tenable Security Center User Guide*.
- (Optional) Restore the configuration backup file, as described in Restore a Configuration Backup.

Restore a Configuration Backup

Required Tenable Security Center User Role: Root user

For more information about the backup and restore process and the configurations included in a configuration backup, see Backup and Restore.

Note: For best performance, after restoring a configuration backup, ensure the hostname associated with the configuration backup file matches the hostname on the receiving Tenable Security Center Director.

Before you begin:

- Perform a configuration backup of your Tenable Security Center Director, as described in Perform a Configuration Backup.
- Confirm your receiving Tenable Security Center Director meets the requirements described in Backup and Restore.
- If needed, restore configuration backups for your managed Tenable Security Center instances, as described in Restore a Configuration Backup in the *Tenable Security Center User Guide*.

To restore a configuration backup file:

1. Log in to Tenable Security Center Director via the command line interface (CLI).
2. Stop Tenable Security Center Director, as described in Start, Stop, or Restart Tenable Security Center Director.

   Tenable Security Center Director stops.
3. Start PostgreSQL with the following command:

```
su - tns
/opt/sc/support/bin/pg_ctl -D /opt/sc/data/postgresql/ -l
/opt/sc/admin/logs/postgresql.log start
exit
```

> **Note:** If you are using an external PostgreSQL server, the server must be up and running before you continue to the next step.

4. In the CLI in Tenable Security Center Director, run the following command to restore the configuration backup, where [*path to backup file*] is the path to the backup file you want to restore:

   ```
   /opt/sc/support/bin/php /opt/sc/src/tools/restoreSCConfiguration.php -l [path to backup file]
   ```

   For example:

   ```
   /opt/sc/support/bin/php /opt/sc/src/tools/restoreSCConfiguration.php -l /tmp/SC-config-20211101-165111-sc-hostname-5_20_0.tar.gz
   ```

   Tenable Security Center Director restores the configuration backup.

5. Start Tenable Security Center Director, as described in Start, Stop, or Restart Tenable Security Center Director.

   Tenable Security Center Director starts.

What to do next:

1. Review your Nessus scanners and scan zones. Tenable Security Center Director restores Nessus scanner and scan zone data from the configuration backup. However, Tenable Security Center Director clears the credentials for each restored Nessus scanner, including when you restore to a new installation with the same hostname, because the configuration backup does not include the encryption key and the encryption keys differ between Tenable Security Center Director instances. To make each scanner functional again, re-enter its credentials. The system log (System Logs) records a warning that the credentials could not be decrypted and were cleared. For more information, see Tenable Nessus Scanners and Scan Zones.
2. If you restored the configuration backup to a new Tenable Security Center Director installation, apply your license, as described in Apply a New License. Until you apply a license, users see a

"License is invalid" error. The configuration backup does not include license keys.

3. If you uploaded custom plugins before restoring your Tenable Security Center Director configuration, re-upload the custom plugins. For more information, see Custom Plugin Packages for NASL and CA Certificate Upload.
4. Perform discovery scans on your managed Tenable Security Center instances to re-populate your repositories with vulnerability data. For more information, see Scanning Overview.

Monitor Scans

See the following sections to monitor scans running on your managed Tenable Security Center instances.

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 Security Center Director scanning strategies, see the Tenable Security Center Scan Tuning Guide.

In Tenable Security Center Director, you can monitor the scans running on your managed Tenable Security Center instances. Tenable Security Center Director cannot run scans.

Tip: You can manage scan policy configurations for active scans on your managed Tenable Security Center instances from Tenable Security Center Director using the Tenable Security Center Director API. For more information, see the *Tenable Security Center API Guide*.

Scan Type	Description	Licensing
Discovery Scan	Find assets on your network. For example: • a scan configured with the **Host Discovery** template. • a scan configured to use only discovery plugins. • an Tenable Network Monitor instance in discovery mode.	Assets identified by discovery scans do not count toward your license.

Assessment Scan	Find vulnerabilities on your assets. For example: • an *authenticated* or *unauthenticated* active scan using a Tenable Nessus or Tenable One Vulnerability Management scanner. • an agent scan using an agent-capable Tenable One Vulnerability Management or Tenable Nessus Manager scanner. **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	In general, assets assessed by assessment scans count toward your license.

	scan configuration, Tenable One Vulnerability Management 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 Security Center instances.

Tenable 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.

Tenable Nessus Scanners

In the Tenable Security Center framework, the Tenable Nessus scanner behaves as a server, while Tenable Security Center serves as a client that schedules and initiates scans, retrieves results, reports results, and performs a wide variety of other important functions.

If your deployment includes Tenable Security Center Director, you can use it to manage the Tenable Nessus scanners on your managed Tenable Security Center instances.

You can add managed or unmanaged Tenable Nessus deployments to Tenable Security Center as Tenable Nessus scanners in Tenable Security Center.

Note: Tenable Security Center cannot perform scans with or update plugins for scanners running unsupported versions of Tenable Nessus. For minimum Tenable Nessus scanner version

requirements, see the Tenable Security Center Release Notes for your version.

For more information, see:

For information about Tenable Security Center-Tenable Nessus communications encryption, see Encryption Strength.

Tenable Nessus Scanner Settings

Option	Description
General	
Tenable Security Center Instance	The name of the managed Tenable Security Center instance where you configured the Tenable Nessus scanner.
Name	A descriptive name for the scanner.
Description	A scanner description, location, or purpose.
Host	The hostname or IP address of the scanner.
Port	The TCP port that the scanner listens on for communications from Tenable Security Center. The default is port 8834.
Enabled	A scanner may be **Enabled** or **Disabled** within Tenable Security Center to allow or prevent access to the scanner. **Note:** Disabling a Tenable Nessus scanner also suspends plugin updates on that scanner.
Verify Hostname	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.

Option	Description
	Note: Confirm that the correct CA certificate is configured for use by Tenable Security Center. If you are using a custom CA, configure Tenable Security Center 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 Tenable Nessus servers.
Use Proxy	Instructs Tenable Security Center to use its configured proxy for communication with the scanner.
Authentication	
Type	Select **Password**, **SSL Certificate**, or **API Keys** for the authentication type to connect to the scanner. For complete information about Tenable Nessus SSL certificate authentication, see Manual Nessus SSL Certificate Exchange.
Username	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 Security Center, a standard user account may be used to perform scans. This option is only available if the **Authentication Type** is set to **Password**.
Password	The login password must be entered in this option. This option is only available if the **Authentication Type** is set to **Password**.
Certificate	If you set **Authentication Type** to **SSL Certificate**, specifies the `nessuscert.pem` file you want to use for authentication to the scanner. For complete information about Tenable Nessus SSL certificate authentication, see Manual Nessus SSL Certificate Exchange.

Option	Description
Certificate Passphrase	If you selected **SSL Certificate** as the **Authentication Type** and the private key that decrypts your SSL certificate is encrypted with a passphrase, the passphrase for the private key.
Active Scans	
Zones	The scan zones that can use this scanner. For more information, see Scan Zones.
Agents	
Agent Capable	Specifies whether you want this scanner to provide Tenable Agent scan results to Tenable Security Center. Agent capable scanners must be Tenable Nessus Manager 6.5 or later. When using Tenable Nessus Manager, you must connect from Tenable Security Center using an administrator or organizational user account. For more information, see User Roles. **Note:** Tenable Security Center does not push plugin updates to **Agent Capable** scanners (Tenable Nessus Manager). If plugins do not download automatically from plugins.nessus.org, you must update them manually.
Organizations	When the **Agent Capable** option is enabled, or you select **API Keys** as the **Authentication Type**, specifies one or more organizations that you want to grant access to import Tenable Agent data into Tenable Security Center.
API Keys	When the **Agent Capable** option is enabled, specifies whether you want to use secure API keys when importing agent scan data from Tenable Nessus scanners. For more information about retrieving your access key and secret key from

Option	Description
	Tenable Nessus, see Generate a Nessus API Key in the *Tenable Nessus User Guide* .
Access Key	When the **API Keys** option is enabled, specifies the access key for the Tenable Nessus scanner. When you select **API Keys** as the **Authentication Type**, specifies the access key for the Tenable Agent.
Secret Key	When the **API Keys** option is enabled, specifies the secret key for the Tenable Nessus scanner. When you select **API Keys** as the **Authentication Type**, specifies the secret key for the Tenable Agent.
Web Application Scanning	
Capable	Specifies whether you want this scanner to provide Tenable One Web App Scanning scan results to Tenable Security Center.

Add a Tenable Nessus Scanner

Required Tenable Security Center User Role: Administrator

You can add a Tenable Nessus scanner to a managed Tenable Security Center instance. For more information, see Tenable Nessus Scanners.

Note: Tenable Security Center cannot perform scans with or update plugins for scanners running unsupported versions of Tenable Nessus. For minimum Tenable Nessus scanner version requirements, see the Tenable Security Center Release Notes for your version.

Note: Tenable Security Center does not send plugins to linked Nessus Managers. Nessus Manager pulls plugins directly from Tenable's plugin sites. Therefore, to update plugin sets, Nessus Manager needs access to the internet and Tenable's plugin sites (for more information, see the Which Tenable

sites should I allow? community article). If your Nessus Manager does not have internet access, you can manually update its version and plugins offline (for more information, see Manage Nessus Offline in the *Nessus User Guide*).

To add a Tenable Nessus scanner to a managed Tenable Security Center instance:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Scan Infrastructure**> **Scanners**.

   The **Tenable Nessus Scanners** page appears.
3. At the top of the table, click **Add**.

   The **Add Tenable Nessus Scanner** page appears.
4. Configure Tenable Nessus scanner options, as described in Tenable Nessus Scanners.
   a. In the **Tenable Security Center Instance** drop-down box, select a managed Tenable Security Center instance for the scanner.

      Tip: If you arrived at the **Add Tenable Nessus Scanner** page from the **Scanners** tab on a Tenable Security Center instance details page, you cannot modify the **Tenable Security Center Instance** option.

   b. In the **Name** box, type a name for the scanner.
   c. In the **Description** box, type a description for the scanner.
   d. In the **Host** box, type the hostname or IP address for the scanner.
   e. In the **Port** box, view the default (**8834**) and modify, if necessary.
   f. If you want to disable this scanner's connection to Tenable Security Center, click **Enabled** to disable the connection.
   g. If you want to verify that the hostname or IP address entered in the **Host** option matches the CommonName (CN) presented in the SSL certificate from the Tenable Nessus scanner, click **Verify Hostname** to enable the toggle.
   h. If you want to use the proxy configured in Tenable Security Center Directorfor communication with the scanner, click **Use Proxy** to enable the toggle.
   i. In the **Type** drop-down box, select the authentication type.

j. If you selected **Password** as the **Type**:

i. In the **Username** box, type the username for the account generated during the Tenable Nessus installation for daemon-to-client client communications.

ii. In the **Password** box, type the password associated with the username you provided.

k. If you selected **SSL Certificate** as the **Type**:

i. Click **Choose File** to upload the `nessuscert.pem` file you want to use for authentication to the scanner.

ii. (Optional) If the private key that decrypts your SSL certificate is encrypted with a passphrase, in the **Certificate Passphrase** box, type the passphrase for the private key.

l. Check the box for all active scan zones you want to use this scanner.

m. If you want this scanner to provide Tenable Agent scan results to Tenable Security Center:

i. Click **Agent Capable** to enable the toggle.

ii. Check the box for one or more **Organizations** that you want to grant access to import Tenable Agent data into Tenable Security Center.

iii. If you want to use secure API keys when importing agent scan data from Tenable Nessus scanners:

a. Click **API Keys** to enable the toggle.

b. In the **Access Key** box, type the access key.

c. In the **Secret Key** box, type the secret key.

5. Click **Submit**.

Tenable Security Center Director saves your configuration.

What to do next:

- Configure a scan zone, repository, and active scan objects on the managed Tenable Security Center instance, as described in Active Scans in the *Tenable Security Center User Guide*.

Tenable Nessus Scanner Statuses

You can view the status for scanners, as described in View Your Tenable Nessus Scanners.

Status Code	Status Message	Description	Recommended Action
1	**Working**	The scanner is connected to Tenable Security Center and able to run scans.	None.
2	**Connection Error**	Tenable Security Center cannot connect to the scanner because the scanner is unreachable or does not exist at the IP address or hostname provided.	Do one or both of the following: • Check your scanner configuration and confirm the **Host** option specifies the correct IP address or hostname for the scanner. • Confirm the network devices and firewalls between Tenable Security Center and the scanner are configured to permit network traffic.
4	**Connection Timeout**	Tenable Security Center connected to the scanner but timed out waiting for a reply.	Contact your network administrator for troubleshooting assistance.

Status Code	Status Message	Description	Recommended Action
8	**Certificate Mismatch**	Tenable Security Center could not confirm the validity of the SSL certificate presented by the scanner.	Do one of the following: • Edit your scanner configuration and select a different authentication type. • (Tenable Nessus scanners only) Check your scanner configuration settings and confirm the **Certificate** option specifies the correct `nessuscert.pem` file. For more information about managing SSL certificates in Nessus, see Manage SSL Certificates in the *Tenable Nessus User Guide*.
16	**Protocol Error**	Tenable Security Center connected to the scanner but the scanner returned an HTTPS protocol negotiation error.	Contact your network administrator for troubleshooting assistance.
32	**Authentication**	Tenable Security Center	Check your scanner

Status Code	Status Message	Description	Recommended Action
	Error	could not authenticate to the scanner using the credentials you provided.	configuration settings and confirm the **Username** and **Password** options specify valid login credentials for the scanner.
64	**Invalid Configuration**	The scanner attempted to connect to a scanner on port 0, or the provided API key is for a scanner that does not support agent scans.	Do one or both of the following: • Check your scanner configuration and confirm the **Port** option specifies a valid TCP port to connect to your scanners. For more information, see Port Requirements. • Check your scanner configuration and confirm the **Access Key** and **Secret Key** options specify valid keys for a Tenable Nessus Manager or cloud scanner.
128	**Reloading Scanner**	The scanner is temporarily unable to run scans because Tenable	None.

Status Code	Status Message	Description	Recommended Action
		Nessus is restarting on the scanner.	
256	**Plugins Out of Sync**	The plugin sets on the scanner do not match the plugin sets in Tenable Security Center.	For troubleshooting assistance, see the knowledge base article.
1024	**Updating Plugins**	Tenable Security Center is performing a plugin update on the scanner.	You may want to schedule plugin updates to run a few hours before your scheduled scans. For more information, see Edit Plugin and Feed Settings and Schedules. If a scanner has a persistent **Updating Plugins** status, the plugin update have been interrupted. For troubleshooting assistance, see the knowledge base article.
8192	**Updating Status**	Tenable Security Center is refreshing the status of the scanner. Scanners can continue to run scans while Tenable Security Center refreshes the	None.

Status Code	Status Message	Description	Recommended Action
		status. **Note:** Tenable Security Center automatically refreshes scanner statuses every 15 minutes. If you create a new scanner, edit a scanner, or manually refresh the status using the **Update Status** option, Tenable Security Center refreshes the status of the scanner on demand.	
16384	**User Disabled**	A Tenable Security Center user disabled the scanner.	Edit your scanner configuration and click the **Enabled** toggle to re-enable the scanner. For more information about scanner options, see Tenable Nessus Scanners.
32768	**Upgrade Required**	The version of Tenable Nessus on the scanner is unsupported and requires an upgrade. Tenable Security Center	Upgrade to a supported version of Tenable Nessus, as described in Upgrade Nessus in the *Tenable Nessus User Guide*.

Status Code	Status Message	Description	Recommended Action
		cannot perform scans with or update plugins for scanners running unsupported versions of Tenable Nessus. For minimum Tenable Nessus scanner version requirements, see the Tenable Security Center Release Notes for your version.	
131072	**License Invalid**	Missing or invalid license file.	Upload or register a new license through the admin UI or API.
1048576	**Fingerprint Mismatch**	The UUID that a scanner (Tenable Nessus) returned during a status check doesn't match the UUID that Tenable Security Center Director has stored for that scanner.	Remove and re-add the scanner in the Tenable Security Center Director UI — this clears the stored UUID and re-registers with the scanner's current UUID.
2097152	**Permission Error**	The provided API keys do not have the correct permissions to run agent scans.	Check your scanner configuration and confirm the **Access Key** and **Secret Key** options specify valid keys for the scanner.

Manage Nessus Scanners

Required Tenable Security Center User Role: Administrator

Administrators can view and manage Tenable Nessus scanner configurations from the Tenable Security Center user interface. For more information about Tenable Nessus scanners in Tenable Security Center, see Tenable Nessus Scanners.

View Your Tenable Nessus Scanners

You can view the Tenable Nessus scanners on your managed Tenable Security Center instances.

To view a list of configured Tenable Nessus scanners on your managed Tenable Security Center instances:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Scan Infrastructure** > **Tenable Nessus Scanners**.

   The **Tenable Nessus Scanners** page appears.
3. View details about each Tenable Nessus scanner.
   - **Name** – The name for the scanner.
   - **Tenable Security Center Instance** – The name of the Tenable Security Center instance where the scanner is configured. For more information, see Tenable Security Center Director Deployments.
   - **Features** – Specifies whether the scanner is a **Standard** scanner or an **Agent Capable** scanner. Agent capable scanners provide Tenable Agent scan results to Tenable Security Center.
   - **Status** – The status of the scanner. For more information, see Tenable Nessus Scanner Statuses.
   - **Host** – The IP address or hostname of the scanner.
   - **Version** – The scanner's Tenable Nessus version.

- **Type** – The type of scanner connection.

Type	Description
Unknown	Tenable Security Center could not identify the scanner.
Nessus (Unmanaged Plugins)	Tenable Security Center accesses the scanner using a Tenable Nessus user account with **Standard** permissions. Tenable Security Center cannot send plugin updates to the scanner or manage the scanner's activation code.
Nessus (Managed Plugins)	Tenable Security Center manages the scanner and authenticates via a Tenable Nessus user account. Tenable Security Center sends plugin updates to the scanner and manages the scanner's activation code.

- **Uptime** – The value indicates the number of days or the amount of time the scanner has been active. This duration corresponds to the Nessus service (nessusd) process running time.
- **Last Modified** – The date and time the scanner was last modified.

4. To view details of a specific Tenable Nessus scanner, see View Details for a Tenable 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, at the top of the table, click **Update Status**.

   Tenable Security Center Director refreshes the **Status** data.

View Details for a Tenable Nessus Scanner

To view details for a Tenable Nessus scanner:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Scan Infrastructure** > **Tenable Nessus Scanners**.

   The **Tenable Nessus Scanners** page appears.
3. Right-click the row for the scanner you want to view.

   The actions menu appears.

   -or-

   Select the check box for the scanner you want to view.

   The available actions appear at the top of the table.
4. Click **View**.

   The **View Tenable Nessus Scanner** page appears.

Section	Action
Options drop-down box	• To edit the scanner, click **Edit**. • To delete the scanner, click **Delete**, as described in Delete a Tenable Nessus Scanner. • To download logs for the scanner, click **Download Logs**. For more information, see Manage Nessus Scanners.
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**. • **Organizations** – If the scanner is agent capable, the

Section	Action
	organization configured for the scanner. • **API Keys Set** – If the scanner is agent capable, specifies whether API keys are configured for the scanner: **Yes** or **No**.
Data summary	View metadata and performance metrics for the scanner. **Note:** Tenable Security Center Director refreshes the load information every 15 minutes.
Nessus Scanner Health	If you are viewing details for a managed Tenable 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 Security Center last updated the scanner data.

Section	Action
	Tenable Security Center refreshes the data when you load the **View Nessus Scanner** page. To force a manual refresh, click the  button.

Edit a Tenable Nessus Scanner

To edit a Tenable Nessus scanner on your managed Tenable Security Center instance:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Scan Infrastructure** > **Scanners**.

   The **Tenable Nessus Scanners** page appears.
3. Right-click the row for the scanner.

   The actions menu appears.

   -or-

   Select the check box for the scanner.

   The available actions appear at the top of the table.
4. Click **More** > **Edit**.

   The **Edit Tenable Nessus Scanner** page appears.
5. Modify the scanner options. For more information about scanner options, see Tenable Nessus Scanners.

   > **Note:** You cannot move a scanner from one managed Tenable Security Center instance to another. To change the **Tenable Security Center Instance**, delete the scanner and add a new scanner with the same settings on a different Tenable Security Center instance.
6. Click **Submit**.

Delete a Tenable Nessus Scanner

You can delete a Tenable Nessus scanner to permanently remove it from a managed Tenable Security Center instance.

To delete a Tenable Nessus scanner from a managed Tenable Security Center instance:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Scan Infrastructure**> **Scanners**.

   The **Nessus Scanners** page appears.
3. Select the scanner you want to delete:
   - To delete a single scanner:
     a. In the table, right-click the row for the scanner you want to delete.

        The actions menu appears.

     b. Click **Delete**.
   - To delete multiple scanners:
     a. In the table, select the check box for each scanner you want to delete.

        The available actions appear at the top of the table.

     b. At the top of the table, click **More** > **Delete**.

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

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

   Tenable Security Center Director deletes the scanner from the managed Tenable Security Center instance.

Pause, Resume, or Stop Scans on a Managed Tenable Security Center Instance

Required Tenable Security Center Director User Role: Administrator

From Tenable Security Center Director, you can pause, resume, and stop scans that are running on managed Tenable Security Center 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 Security Center instances to Tenable Security Center Director, see Tenable Security Center Director Deployments.

To pause, resume, or stop scans on a managed Tenable Security Center instance:

1. Log in to Tenable Security Center 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 ⏸ button.

     Tenable Security Center pauses the scan on the managed Tenable Security Center instance.
4. To resume a paused scan:
   - In the row for the scan you want to resume, click the ▶ button.

     Tenable Security Center resumes the paused scan on the managed Tenable Security Center instance.
5. To stop a running scan:
   a. In the row for the scan you want to stop, click the ⚙ menu.

      The actions menu appears.
   b. Click **Stop**.
   c. Click one of the following options to determine how the managed Tenable Security Center instance handles the results of the stopped scan:
      - **Discard Results** – The managed Tenable Security Center instance does not import any of the results obtained by the scan to the database.

- **Import Results** – The managed Tenable Security Center instance imports the results of the current scan and discards the information for the unscanned hosts.
- **Import Results and Create Rollover** – The managed Tenable Security Center 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 Security Center stops the scan on the managed Tenable Security Center instance.

Repositories

Repositories are databases within Tenable Security Center 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 Security Centers.

> **Note:** The maximum repository size is 64 GB. For best performance, Tenable recommends splitting repositories larger than 32 GB (greater than 50% capacity).

When adding an *external repository*, you access a local repository from another Tenable Security Center.Remote repositories allow you to share repository data from one Tenable Security Center deployment to your primary Tenable Security Center deployment via an SSH session. By default, Tenable Security Center Director uses ECDSA keys for remote repository authentication.

External repository data is static and used solely for reporting purposes. For more information, see External Repositories.

> **Note:** Each repository is a separate entity that stores data independently. Mitigation occurs within each repository separately.

For more information, see Manage Repositories. For information about Tenable Security Center 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.

For information about how Tenable Security Center Director tracks vulnerability data over time in dashboards and reports, see Trending.

Manage Repositories

Required Tenable Security Center User Role: Administrator

Note: By default, Tenable Security Center Director uses ED25519 keys for remote repository authentication regardless of FIPS mode settings.

For more information, see Repositories.

Add a Repository

To add a repository:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Repositories**.

   The Repositories page appears.
3. At the top of the table, click **Add**.

   The **Add Repository** page appears.
4. Click the tile for the repository type you want to add.

   The **Add Repository** page appears.
5. Configure the options for your repository. For more information, see Remote Repositories.
6. Click **Submit**.

   Tenable Security Center Director saves your configuration.

View Your Repositories

To view a list of your repositories:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Repositories** > **Repositories**.

   The **Repositories** page appears.
3. (Optional) To filter the repositories that appear on the page, apply a filter as described in Apply a Filter.
4. View details about each repository.
   - **Name** – The name of the repository.
   - **Vulnerability Count** – The total number of vulnerability instances in the repository.

     > **Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

   - **IP/Device Count** – The total number of assets for which the repository contains vulnerability data.
   - **Type** – The repository type.
   - **Capacity** – (Asset repositories only) The percentage of maximum available repository space you are currently using. The maximum repository size is 64 GB.

     > **Tip:** For best performance, Tenable recommends splitting repositories larger than 32 GB.

   - **Last Updated** – The date and time the repository was last updated.

View Repository Details

To view repository details:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Repositories** > **Repositories**.

   The **Repositories** page appears.

3. (Optional) To filter the repositories that appear on the page, apply a filter as described in Apply a Filter.
4. Right-click the row for the repository you want to view.

   The actions menu appears.

   -or-

   Select the check box for the repository you want to view.

   The available actions appear at the top of the table.
5. Click **View**.

   The **View Repository** page appears.

Section	Action
General	View general information for the repository. • **Name** – The repository name. • **Description** – The repository description. • **IP Count** – The total number of assets for which the repository contains vulnerability data. • **Last Vuln Update** – The date and time the repository was last updated. • **Vulnerability Count** – The total number of vulnerability instances in the repository. **Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol. • **Repository Capacity** – (Asset repositories only) The percentage of maximum available repository space you are currently using. The maximum repository size is 64 GB.

Section	Action
	Tip: For best performance, Tenable recommends splitting repositories larger than 32 GB. • **Created** – The date the repository was created. • **Last Modified** – The date the repository was last modified. • **ID** – The repository ID.
Data	View a summary of the repository data (for example, the IP address range). For more information, see Remote Repositories.
Access	View the name of the organizations with access to this repository.
Advanced Settings	View a summary of your settings for the repository. For more information about a setting, see Remote Repositories.

Edit a Repository

To edit a repository:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Repositories** > **Repositories**.

   The **Repositories** page appears.
3. (Optional) To filter the repositories that appear on the page, apply a filter as described in Apply a Filter.
4. Right-click the row for the repository you want to edit.

   The actions menu appears.

   -or-

   Select the check box for the repository you want to edit.

   The available actions appear at the top of the table.

5. Click **More** > **Edit**.

   The **Edit Repository** page appears.

6. Modify the repository options, as described in Remote Repositories.
7. Click **Submit**.

   Tenable Security Center Director saves your configuration.

Export a Repository

You can export a repository from one Tenable Security Center and import it as an offline repository on another Tenable Security Center. You can export repositories via the Tenable Security Center user interface or the CLI. 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.

Export via the User Interface

To export a repository via the user interface:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Repositories** > **Repositories**.

   The **Repositories** page appears.

3. Right-click the row for the repository you want to export.

   The actions menu appears.

   -or-

   Select the check box for the repository you want to export.

   The available actions appear at the top of the table.

4. Click **Export**.

   Tenable Security Center Director exports the repository.

Export via the CLI

To export a repository via the CLI:

1. Log in to Tenable Security Center Director via the command line interface (CLI).
2. Prepare the command you want to run.

```
sh /opt/sc/customer-tools/exportRepository.sh [repID] [trendingDays]
[trendWithRaw]
```

Variable	Description
repID	The repository ID of the repository you want to export. To locate the repository ID, view the details for the repository, as described in View Your Repositories.
trendingDays	(IP, Agent, and Universal repositories only) The number of days of vulnerability trending data to include. To use the preconfigured repository setting, type **default**. **Note:** The number of days of trending data included in the export cannot exceed the **Days Trending** setting for the repository or the number of days of trending data available for the repository. For example, if you request 30 days of trending data, but trending data has been enabled for only 15 days, then the export includes only 15 days of trending data. For more information about repository settings, see Asset Repositories.
trendWithRaw	(IP, Agent, and Universal repositories only) Specify whether you want the export to include plugin output data: **yes** or **no**. To use the preconfigured repository setting, type **default**.

(Optional) To automatically overwrite an existing repository file with the same name, include the optional argument `-f`.

3. In the CLI in Tenable Security Center Director, run the export command.

   For example:

```
/opt/sc/customer-tools/exportRepository.sh -f 1 default default
```

Tenable Security Center Director exports the repository.

Delete a Repository

To delete a repository:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Repositories** > **Repositories**.

   The **Repositories** page appears.
3. Select the repository you want to delete:
   - To delete a single repository:
     a. In the table, right-click the row for the repository you want to delete.

        The actions menu appears.

     b. Click **Delete**.
   - To delete multiple repositories:
     a. In the table, select the check box for each repository you want to delete.

        The available actions appear at the top of the table.

     b. At the top of the table, click **More** > **Delete**.

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

   Tenable Security Center Director deletes the repository.

External Repositories

An *external repository* lets you access a local repository from another Tenable Security Center deployment for reporting purposes. External repository data is read-only. You cannot use an external repository as the **Import Repository** for active scans.

About Remote Repositories

Remote repositories allow you to share repository data from one Tenable Security Center deployment to your primary Tenable Security Center deployment via an SSH session. By default, Tenable Security Center Director uses ECDSA keys for remote repository authentication.

Task	Remote Repository
Data transfer	Automatic – Tenable Security Center syncs data over SSH on a configured schedule.
Typical use case	Networked deployments where both instances can communicate over SSH. For large enterprise deployments, see Tiered Remote Repositories.
Version requirement	Both Tenable Security Center deployments must run the same version.
Data freshness	Updated automatically on the configured schedule.
Key limitation	Both deployments must be reachable over SSH. Requires an ed25519 SSH key for authorization (see Caution below).

Caution: Tenable Security Center Director 6.8 uses an updated SSH library. When you update to Tenable Security Center Director 6.8 or later, you must add an ed25519 key for authorization to successfully sync remote repositories. If you do not add the new key, synchronization of your remote repositories will fail.

Configure a Remote Repository

To fully configure a remote repository:

1. Add a remote repository to your primary Tenable Security Center deployment, specifying the IP address of the remote instance.

2. When prompted, provide credentials for an administrator account on the remote Tenable Security Center. The deployments exchange SSH keys and the available repositories populate automatically.
3. Select the repository to sync and configure the update schedule.

For more information, see Remote Repositories, Repositories, and Add a Repository.

Remote Repositories

Caution: Tenable Security Center Director 6.8 uses an updated SSH library. When you update to Tenable Security Center Director 6.8 or later, you must add an ed25519 key for authorization to successfully sync remote repositories. This new requirement ensures that data transmission is secured using the latest cryptographic standards. If you do not add the new key, the synchronization of your remote repositories will fail.

Remote repositories allow you to share repository data from one Tenable Security Center deployment to your primary Tenable Security Center deployment via an SSH session. By default, Tenable Security Center Director uses ECDSA keys for remote repository authentication.

Note: You cannot set a remote repository as the **Import Repository** for active scans. You can use remote repository data only for reporting purposes.

Note: Ensure all your Tenable Security Center Director deployments are running the same version. For example, if your remote repository exists on a Tenable Security Center Director running a later version than your primary Tenable Security Center Director deployment, upgrade your primary Tenable Security Center Director deployment to the same version.

For more information, see Manage Repositories.

To use tiered remote repositories for large enterprise deployments of Tenable Security Center, see Tiered Remote Repositories.

Option	Description
General	

Option	Description
Name	The repository name.
Description	(Optional) A description for the repository.
Remote Tenable Security Center	
Host	The IP address for the host you want to synchronize with to obtain repository data. After you type the IP address: 1. Click **Request Repositories**. 2. Type the username and password for an administrator account on the remote Tenable Security Center. The Tenable Security Center deployments exchange SSH keys, and the system populates the **Repository** list with all available repositories from the remote Tenable Security Center.
Repository	The repository on the remote Tenable Security Center instance that you want to synchronize vulnerability data from.
Update Schedule	Sets the schedule for the remote server to be queried for updated information. **Note:** If you use this remote repository as a data source for trending charts, configure the update schedule to sync at least once every 24 hours. Remote repositories that sync less frequently produce gaps in trending data. For more information, see Trending.
Access	
Organizations	Specifies which organizations have access to the vulnerability data stored in the repository.

Option	Description
	If groups are configured for the organization, Tenable Security Center 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.

Active Scan Objects

Complete Tenable Security Center scan configurations rely on the following scan objects. For information about active scans, see Active Scans.

Scan Object	Description
assets	Assets are lists of devices (for example, laptops, servers, tablets, or phones) within a Tenable Security Center organization. You can share assets 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 Asset Tags.
credentials	Credentials are reusable objects that facilitate a login to a scan target. You can configure various types of credentials with different authentication methods for use within scan policies. You can also share credentials between users for scanning purposes. Tenable Security Center supports an unlimited number of SSH, Windows, and database credentials, and four SNMP credential sets per scan configuration. For more information, see Credentials.

audit files	During a configuration audit, auditors verify that your server and device configurations meet an established standard and that you maintain them with an appropriate procedure. Tenable Security Center can perform configuration audits on key assets by using local Tenable Nessus checks that can log directly on to a Unix or Windows server without an agent. Tenable Security Center supports several 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, you can create customized audits for the particular requirements of any organization. You can upload customized audits into Tenable Security Center and make them available to anyone performing configuration audits within an organization. You can upload and use NIST SCAP files in the same manner as an audit file. Navigate to NIST's SCAP website (http://scap.nist.gov) and under the SCAP Content section, download the desired SCAP security checklist zip file. You can then upload the file to Tenable Security Center and select it for use in Tenable Nessus scan jobs. Once you configure audit scan policies in Tenable Security Center, you can use them as needed. Tenable Security Center can also perform audits intended for specific assets. A Tenable Security Center user can use audit policies and asset lists to determine the compliance posture of 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.

Asset Tags

Tenable Security Center Director *asset tags* are lists of devices (for example, laptops, servers, tablets, or phones) within a Tenable Security Center Director organization. Asset Tags can be shared with one or more users based on local security policy requirements.

> **Tip:** For more information about tagging in Tenable products, see the *Tenable Tagging Quick Reference Guide*.

You can add an asset tag to group devices that share common attributes. Then, you can use the asset tag during scan configuration to target the devices in the asset tag. Examples of common attributes include:

- IP address ranges
- hardware types

- vulnerabilities
- outdated software versions
- operating systems

Tenable Security Center Director supports template-based and custom asset tag. For more information about creating and viewing asset tags, see Manage Asset Tags.

To view details about individual hosts that appear in your asset tags, see View Host Details.

> **Note:** When a scan import completes, it queues a job to calculate all dynamic and combination asset tags for the import repository. The next scan import does not begin until the previous scan import asset tag job completes. Usually the asset tag job runs quickly, but delays can occur due to extremely large repositories, a large quantity of asset tags, a backlogged job queue, or other system issues. This does not affect running scans.
>
> Asset tag lists are calculated for each repository, and updating one repository does not affect other repositories.

Template-Based Asset Tags

Tenable provides asset tag templates that you can customize for your environment. Tenable-provided asset tag templates are updated via the Tenable Security Center feed and visible depending on other configurations.

Custom Asset Tags

Tenable Security Center Director supports the following custom asset tag types: Static Asset Tags, DNS Name List Asset Tags, Combination Asset Tags, Dynamic Asset Tags, Watchlist Asset Tags, and Import Asset Tags.

Static Asset Tags

Static asset tags are lists of IP addresses. You can use static asset tags immediately after configuration.

For example, if your organization assigns laptops within a defined IP address range, you can create a custom static asset tag for laptops using that IP address range.

Option	Description
Name	A name for the asset tag.
Description	A description for the asset tag.
Label	A label for the asset tag. For more information, see Labels.
IP Addresses	IP addresses to include within the asset tag (50,000 character limit). • Type a comma-separated list of IP addresses, CIDR addresses, or ranges. • Upload a `.txt` file containing a comma-separated list of IP addressees, CIDR addresses, or ranges.

DNS Name List Asset Tags

Note: You cannot select a DNS name list asset as the target of an agent scan or an agent synchronization job.

Option	Description
Name	A name for the asset tag.
Description	A description for the asset tag.
DNS Names	The DNS hostnames for the asset tag to be based on.

Combination Asset Tags

Combination asset tags allow you to create an asset tag based on existing asset tags and the AND, OR, and NOT operators.

Combination asset tags can include agent IDs if the asset tag contains exclusively dynamic asset tags. You may experience unexpected asset tag behavior if your combination asset tag contains other asset tag types and interacts with agent repository data.

Option	Description
Name	A name for the asset tag.
Description	A description for the asset tag.
Combination	This option accepts multiple existing asset tags utilizing the operators AND, OR, and NOT. You can use these operators and multiple existing asset tags to create new unique asset tags . If the source asset tags change, the **Combination** asset tag updates to match the new conditions. To configure the query: 1. Click inside the **Combination** box. A list of asset tags appears. 2. Click one of the options in the list to select it. 3. Press Space. 4. Continue selecting options and pressing space to describe the combination asset tag you want to configure. **Tip:** A red border around a combination option indicates there is a problem in the query logic.

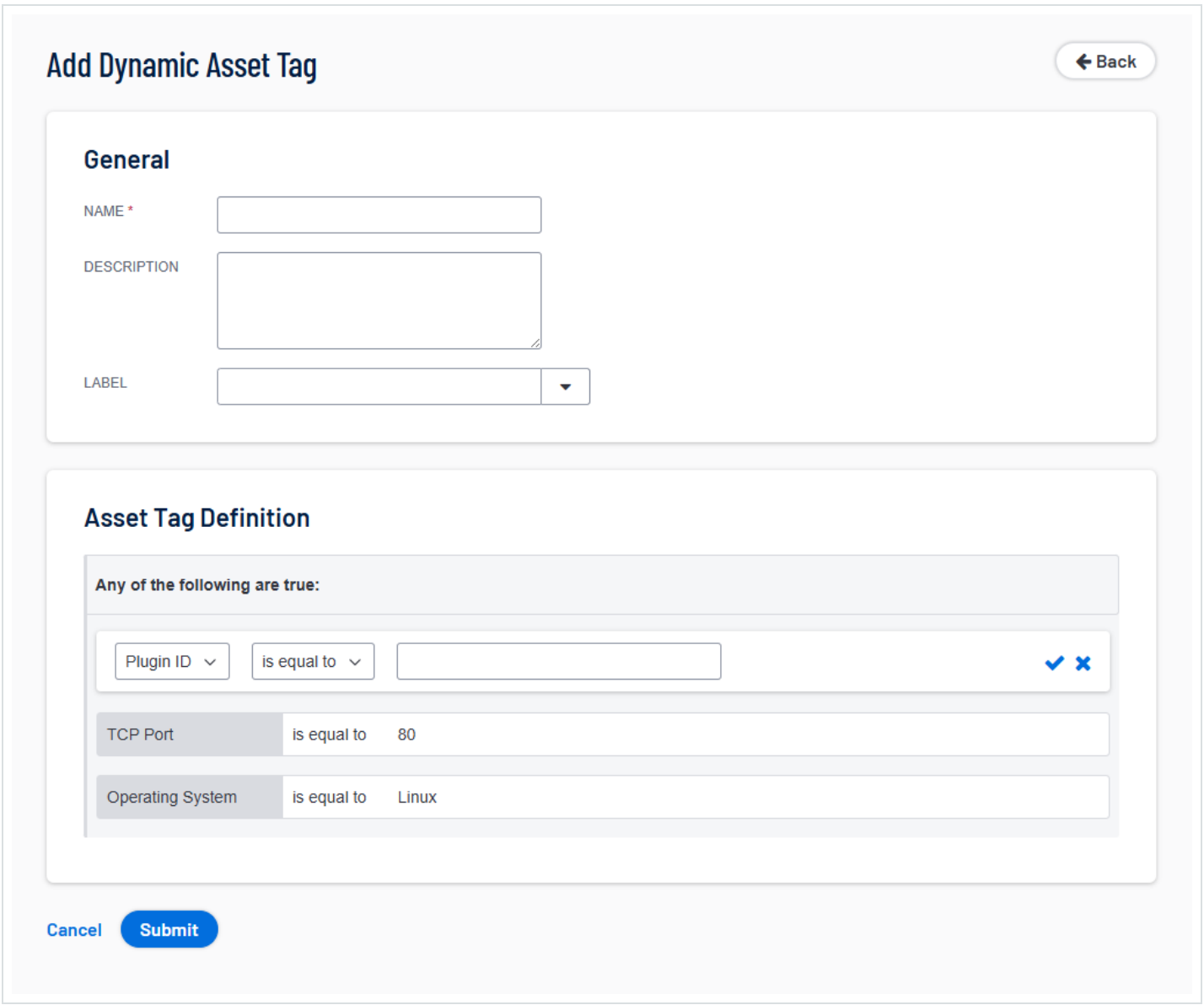
Dynamic Asset Tags

Dynamic asset tags are flexible groups of condition statements that Tenable Security Center Director uses to retrieve a list of devices meeting the conditions. Tenable Security Center Director refreshes dynamic asset tag lists using the results from Tenable Security Center scans. You cannot use dynamic asset tags until after Tenable Security Center performs an initial discovery scan and retrieves a list of devices.

Note: Before a scan can target a dynamic asset tag list, you must first run a host discovery scan in the associated repository. For more information, see the troubleshooting article.

Note: If a dependent scan uses a dynamic asset tag list, the asset list will update before the scan runs.

Dynamic asset tags can include agent IDs.



For example, in the asset tag above, Tenable Security Center Director retrieves a list of Linux systems listening on TCP Port 80.

Option	Description
Name	A name for the asset tag.
Description	A description for the asset tag.

Option	Description
Asset Definition	Defines the rules for creating a dynamic asset tag list. Hover over an existing rule to display the options to add, edit, or delete a group or a rule.

Dynamic Asset Tag Rule Logic

Valid Operators	Effect
Plugin ID	
is equal to	Value must be equal to value specified.
not equal to	Value must be not equal to value specified.
is less than	Value must be less than the value specified.
is greater than	Value must be greater than the value specified.
Plugin Text	
is equal to	Value must be equal to value specified.
not equal to	Value must be not equal to value specified.
contains the pattern	Value must contain the text specified (for example, ABCDEF contains ABC).
Posix regex	Any valid Posix regex pattern contained within “/” and “/” (example: /.*ABC.*/).
Perl compatible regex	Any valid Perl compatible regex pattern.
Operating System	
is equal to	Value must be equal to value specified.

Valid Operators	Effect
not equal to	Value must be not equal to value specified.
contains the pattern	Value must contain the text specified (for example, ABCDEF contains ABC).
Posix regex	Any valid Posix regex pattern contained within “/” and “/” (for example, /.*ABC.*/).
Perl compatible regex	Any valid Perl compatible regex pattern.
IP Address	
Note: The IP Address field accepts a maximum of 1024 characters. This limit applies whether you enter individual IP addresses, CIDR notation, or hyphenated ranges.	
is equal to	Value must be equal to value specified.
not equal to	Value must be not equal to value specified.
DNS, NetBIOS Host, NetBIOS Workgroup, MAC, SSH v1 Fingerprint, SSH v2 Fingerprint	
is equal to	Value must be equal to value specified.
not equal to	Value must be not equal to value specified.
contains the pattern	Value must contain the text specified (for example, 1.2.3.124 contains 124).
Posix regex	Any valid Posix regex pattern contained within “/” and “/” (for example, /.*ABC.*/).
Perl compatible regex	Any valid Perl compatible regex pattern.
Port, TCP Port, UDP Port	

Valid Operators	Effect
is equal to	Value must be equal to value specified.
not equal to	Value must be not equal to value specified.
is less than	Value is less than value specified.
is greater than	Value is greater than the value specified.
Days Since Discovery, Days Since Observation	
is equal to	Value must be equal to value specified (maximum *365*).
not equal to	Value must be not equal to value specified (maximum *365*).
is less than	Value is less than value specified (maximum *365*).
is greater than	Value is greater than the value specified (maximum *365*).
where Plugin ID is	Any valid plugin ID number. You can enter multiple plugin IDs using a range or comma-separated plugin IDs (for example, *3, 10189, 34598, 50000-55000, 800001-800055*).
Severity	
is equal to	Value must be equal to value specified: **Info**, **Low**, **Medium**, **High**, or **Critical**.
not equal to	Value must be not equal to value specified: **Info**, **Low**, **Medium**, **High**, or **Critical**.
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**.

Valid Operators	Effect
where Plugin ID is	Any valid plugin ID number. You can enter multiple plugin IDs using a range or comma-separated plugin IDs (for example, *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 Asset Tags

You can use a watchlist asset tag to maintain lists of IPs that are not in the user's managed range of IP addresses. You can filter for IPs from a watchlist regardless of your IP address range configuration to help analyze 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, you could add it to a Malicious IPs watchlist and to a custom query.

Note: Watchlists only use event data to create the asset tag list.

Option	Description
Name	A name for the asset tag.

Option	Description
Description	A description for the asset tag.
IP Addresses	IP addresses to include within the asset tag list (20,000 character limit). You can enter one address, CIDR address, or range per line. Click **Choose File** to import a list of IP addresses from a saved file.

Import Asset Tags

Option	Description
Name	The asset tag name.
Asset Tag	Click **Choose File** to choose the asset tag that was previously exported for import into Tenable Security Center Director.

Manage Asset Tags

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

Tip: For more information about tagging in Tenable products, see the *Tenable Tagging Quick Reference Guide*.

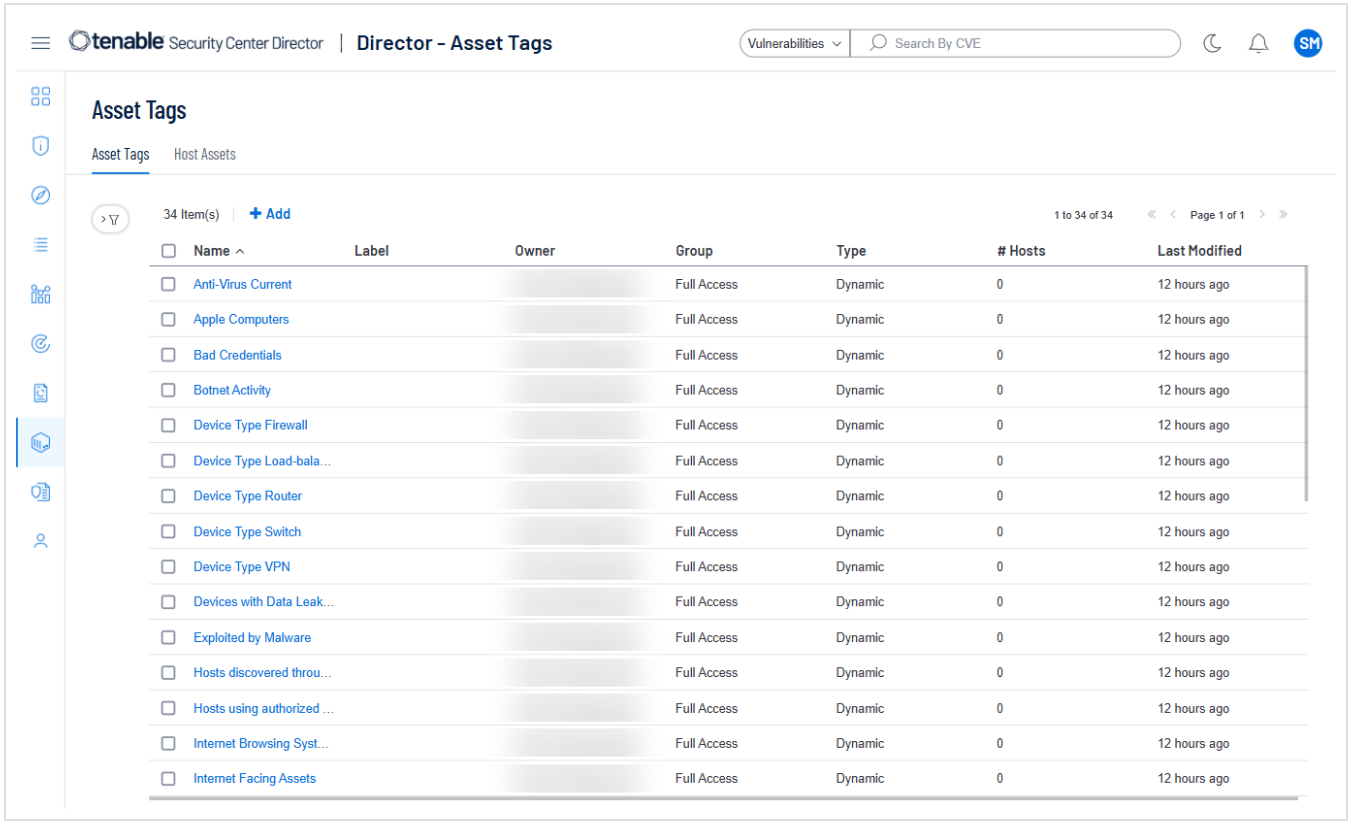
Add a Template-Based Asset Tag

For information, see Asset Tags.

To add an asset tag from a Tenable-provided template:

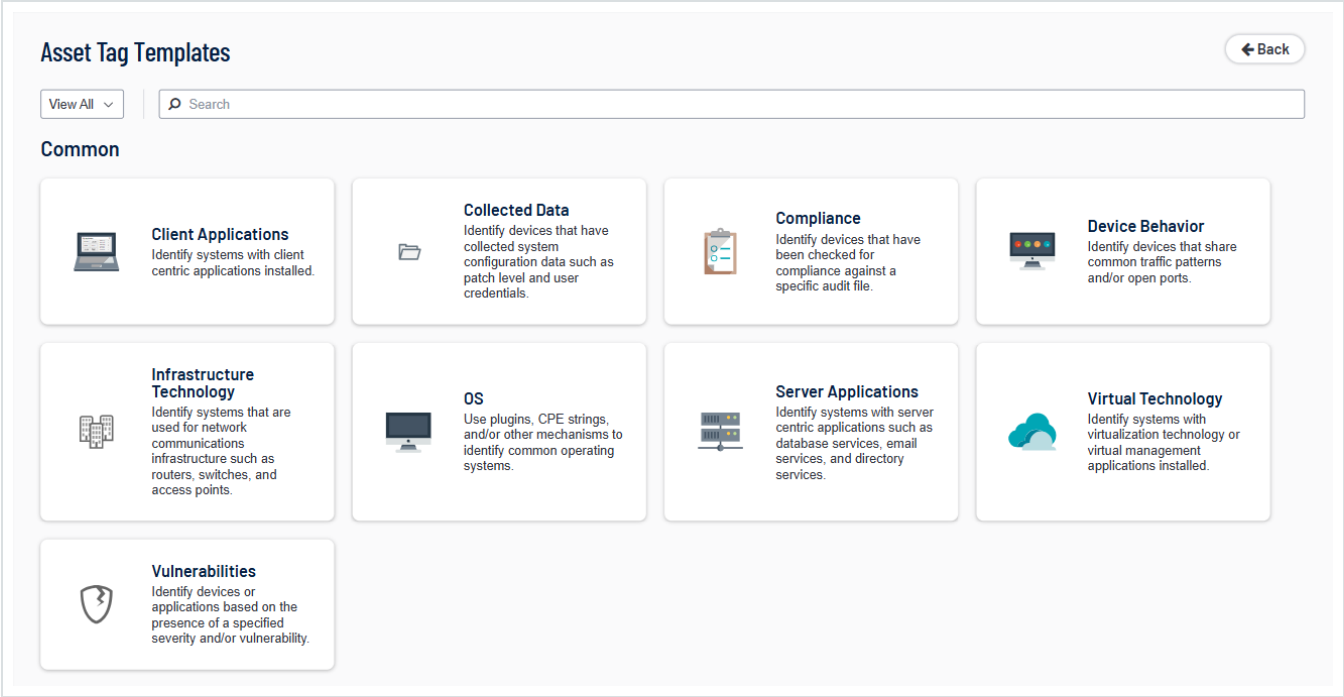
1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, click **Assets** > **Asset Tags**.

The **Asset Tags** page appears.



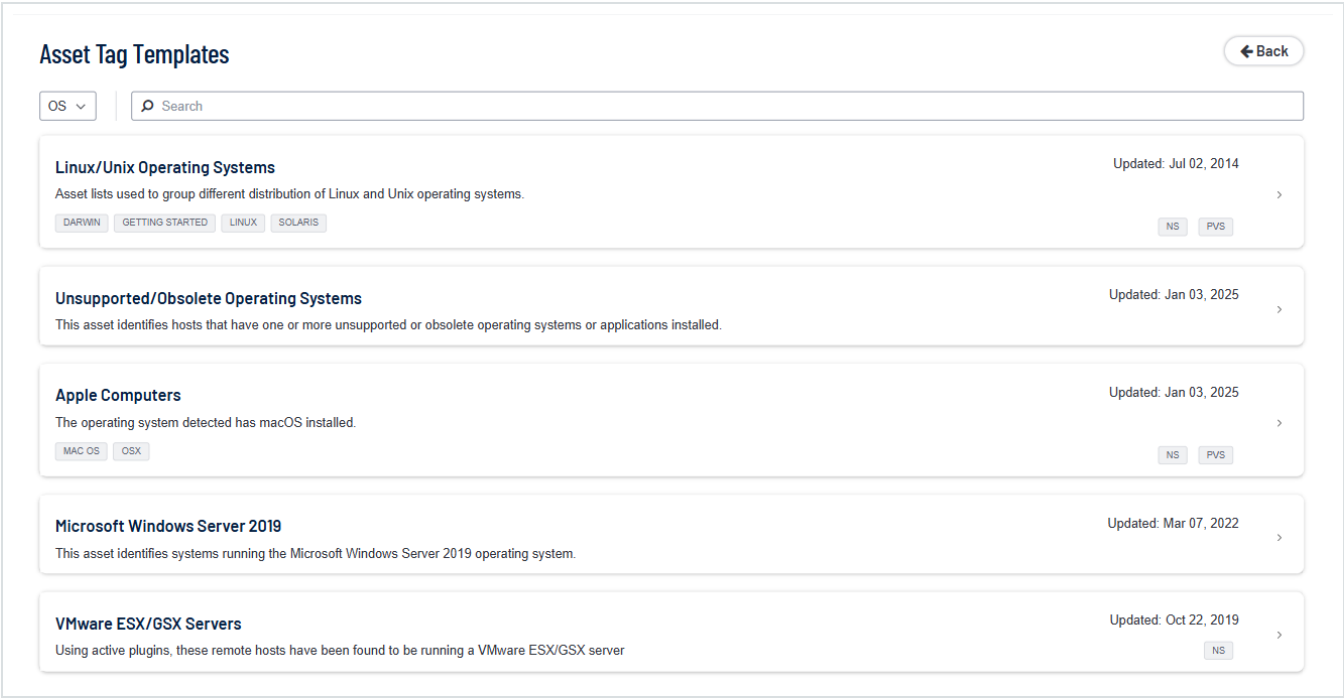
3. At the top of the table, click **Add**.

   The **Asset Tag Templates** page appears.



4. (Optional) If you want to search for a specific asset tag template, type a search phrase in the **Search** box.
5. In the **Common** section, click a template type.

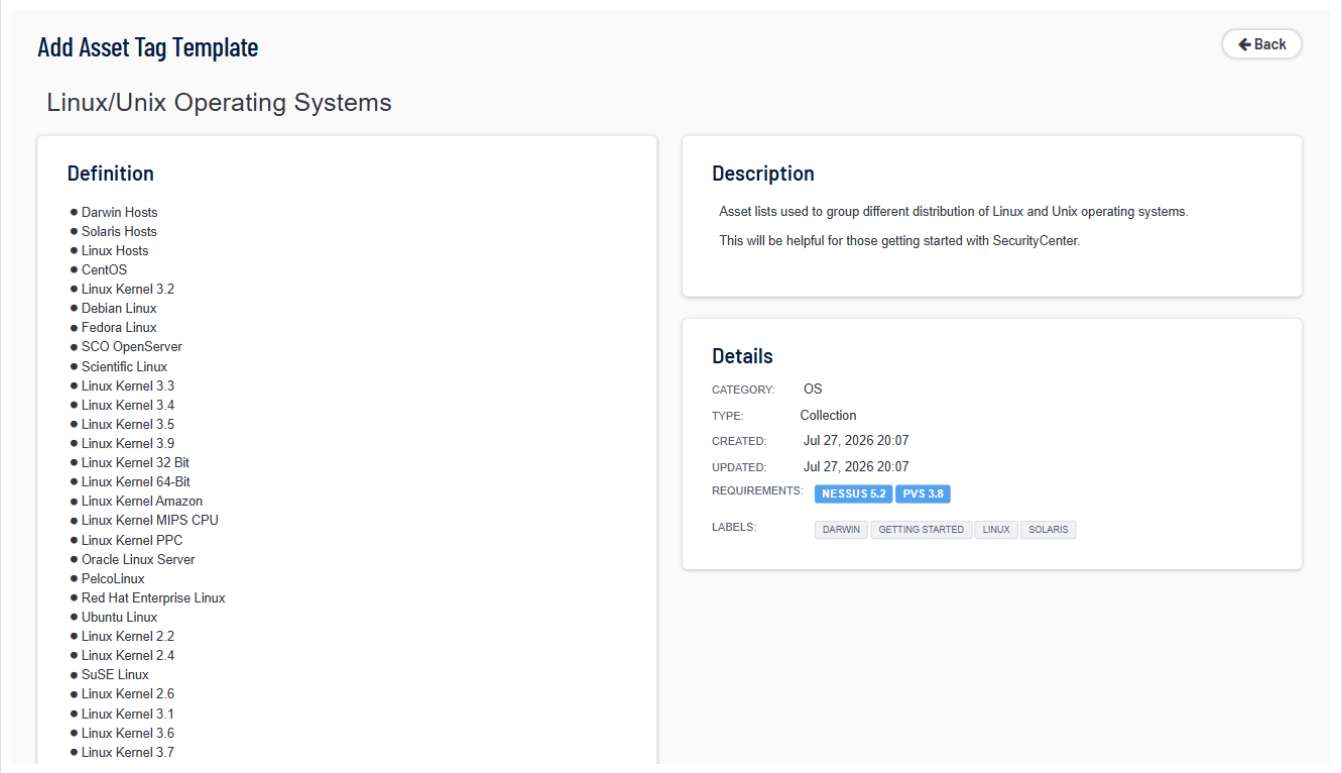
   The **Asset Tag Templates** page for the template type appears.



6. View the available templates.
   - The four square icon ( ) on the left side indicates a collection of several assets.
   - The data icons ( ) on the right side indicate the data required to build the asset.

     The Tenable Network Monitor (PVS) and NS icons indicate you must have Tenable Network Monitor or Tenable Nessus data. The key icon ( ) indicates you must have credentials for the device. The notepad icon ( ) indicates you must have compliance data.
7. (Optional) If you want to search for a specific asset tag template, type a search phrase in the **Search** box or select a category from the **All** drop-down box.
8. Click the row for the template you want to use.

   The **Add Asset Tag Template** page for the template type appears, which displays details about the template.



9. Click **Add**.

   The **Asset Tags** page appears.

10. Click the row for the asset tag you just added.

    The **Edit** page appears.

11. View the details for the asset tag.
12. (Optional) If necessary, edit the asset tag to customize it for your environment. For more information about asset options, see Asset Tags.
13. Click **Submit**.

    Tenable Security Center Director saves your configuration.

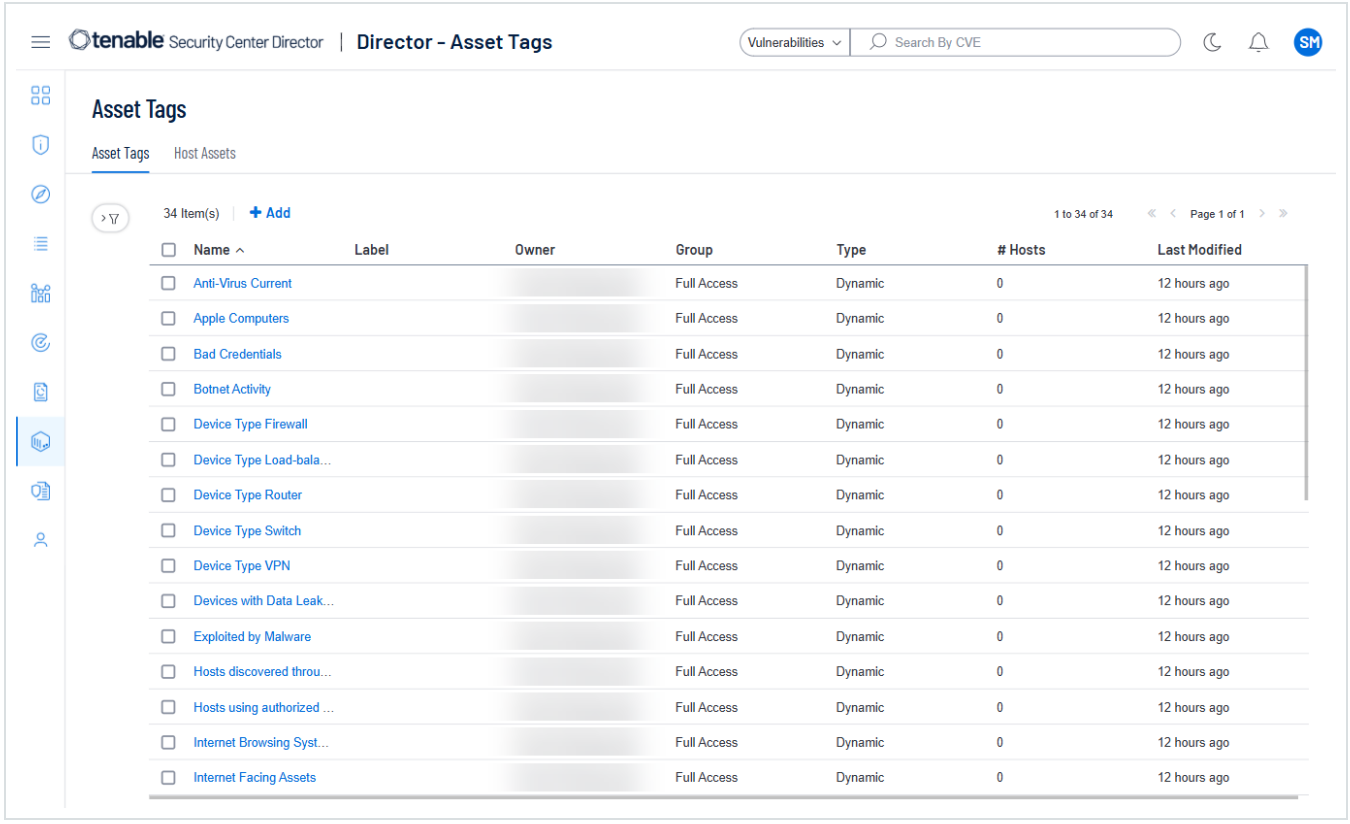
Add a Custom Asset Tag

For information, see Asset Tags.

To add a custom asset tag:

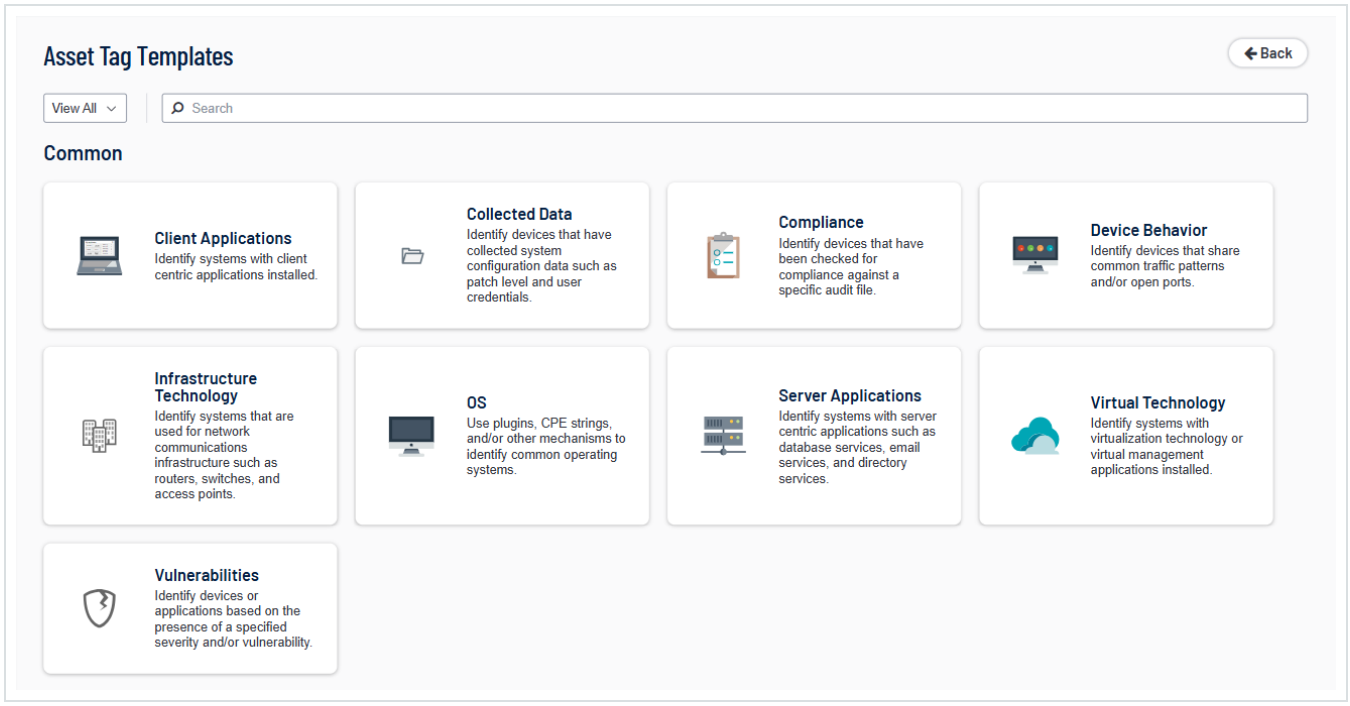
1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, click **Assets** > **Asset Tags**.

   The **Asset Tags** page appears.



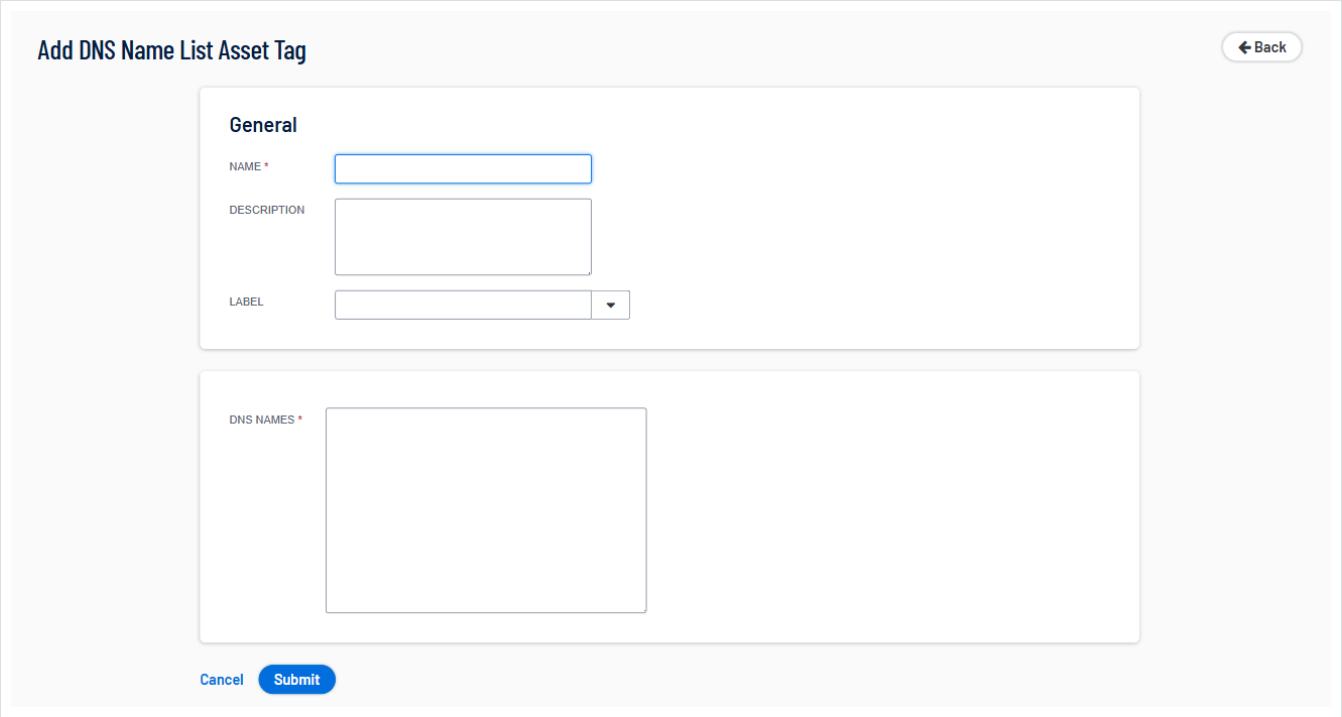
3. At the top of the table, click **Add**.

   The **Asset Tag Templates** page appears.



4. In the **Other** section, click an asset tag type:
    - Static Asset Tags – a list of specific IP addresses, CIDR ranges, or ranges.
    - DNS Name List Asset Tags – a list of DNS hostnames.
    - Asset Tags – a dynamic list built from an LDAP query. Requires a configured LDAP server.
    - Combination Asset Tags – a list built from existing asset tags using AND, OR, and NOT operators.
    - Dynamic Asset Tags – a list built from rule-based conditions evaluated against scan results.
    - Watchlist Asset Tags – a list of IP addresses outside your managed range, used for event analysis.
    - Import Asset Tags – an asset tag imported from a previously exported file.

    The **Add Asset Tag** page for the asset tag type appears.



5. Configure the options for the asset tag type. For descriptions of each option, see Asset Tags.
6. Click **Submit**.

Tenable Security Center Director saves your configuration.

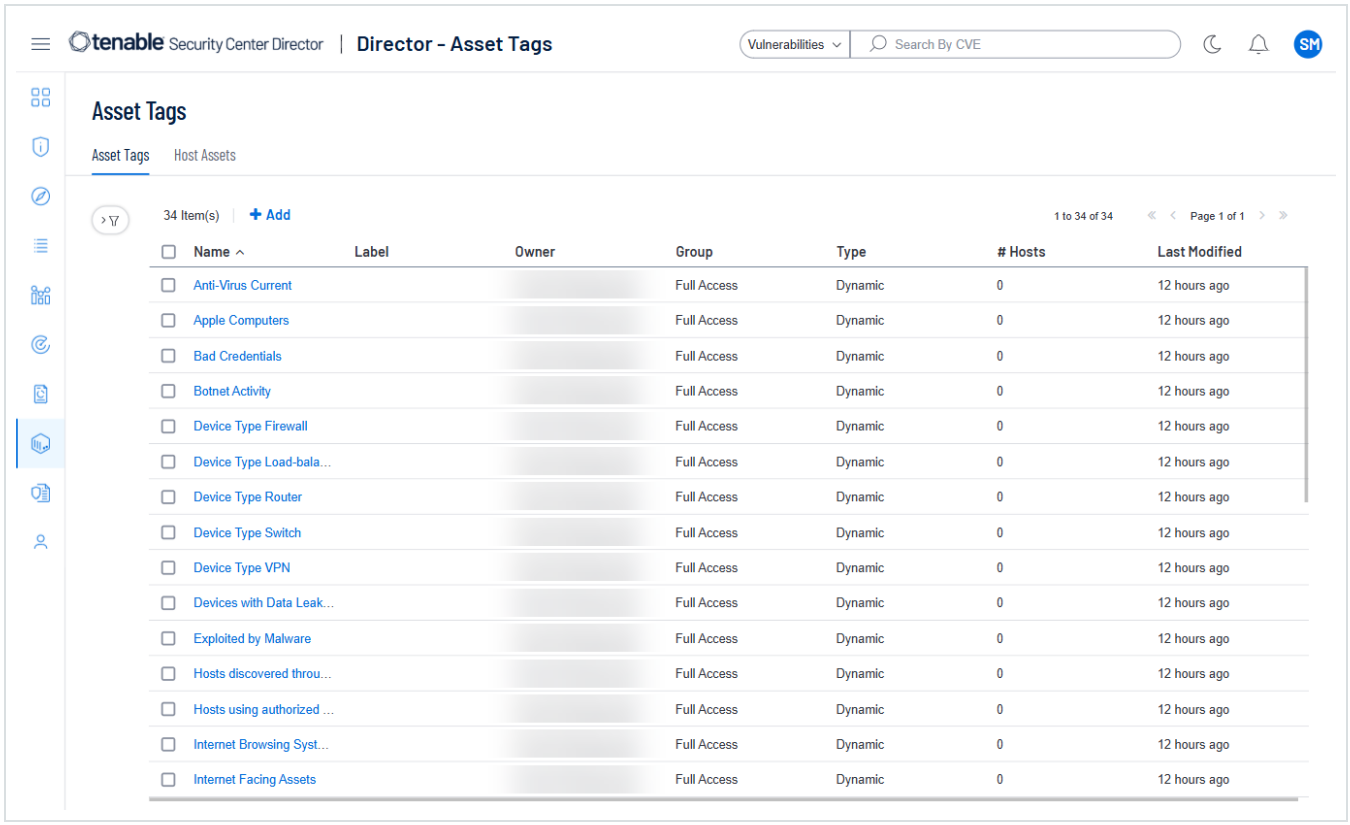
View Asset Tag Details

You can view details for any asset tag. For more information, see Asset Tags.

To view asset tag details:

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, click **Assets** > **Asset Tags**.

   The **Asset Tags** page appears.



3. Right-click the row for the asset tag you want to view.

   The actions menu appears.

   -or-

   Select the check box for the asset tag you want to view.

   The available actions appear at the top of the table.

4. Click **View**.

   The **View Asset Tag** page appears.

Section	Action
General	View general information for the asset tag. • **Name** – The asset tag name. • **Description** – The asset tag description. • **Label** – The label applied to the asset tag. For more information, see Labels. • **IP Addresses** (static asset tags only) – The IP addresses specified in the asset tag. For more information, see Asset Tags. • **Created** – The date the asset tag was created. • **Last Modified** – The date the asset tag was last modified. • **Owner** – The username for the user who created the asset tag. • **Group** – The group in which the asset tag belongs. • **ID** – The asset tag ID.

Manage Hosts

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

View Hosts

You can view a list of hosts associated with asset lists. For more information, see Asset Tags.

To view details for an individual host, see View Host Details.

To view the list of hosts:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Assets** > **Host Assets**.

   The **Host Assets** page appears.
3. (Optional) To filter the list of hosts, apply a filter. For more information, see Host Asset Filter Components.
4. (Optional) To show or hide columns on the **Host Assets** page:
   a. In the table, click the button next to a column header.

      A drop-down menu appears with a list of column names.
   b. Check or uncheck the boxes to show or hide columns.
5. View details about each host asset.
   - **Name** – The name of the host.
   - **AES** – (Requires Tenable Security Center+ license) The host's Asset Exposure Score. For more information, see Asset Exposure Score in the *Tenable One Vulnerability Management User Guide*.
   - **ACR**– (Requires Tenable Security Center+ license) The host's Asset Criticality Rating. For more information, see Asset Criticality Rating in the *Tenable One Vulnerability Management User Guide*.
   - **IP Address** – The host's IP address, if available.
   - **Repository** – The repository that contains vulnerability data associated with the host.
   - **OS** – The operating system running on the host, if available.
   - **System Type** – The host's device type, as determined by plugin 54615.
   - **Net BIOS** – The host's NetBIOS name, if available.
   - **DNS** – The host's DNS name, if available.
   - **Last Seen** – The date and time last Tenable Security Center detected the host on your network.
   - **Asset ID** – The ID of the host.

- **Source** – The type of scan that discovered the host on your network: **Tenable Nessus Scan**, **Tenable Network Monitor**, **Agent Scan**, or **Tenable One OT Exposure Scan**.

> **Tip:** The following columns are hidden by default: **System Type**, **Net BIOS**, **DNS**, and **Asset ID**.

Export Hosts

You can export a list of hosts in a .csv file to share the data with others in your organization. For more information, see Asset Tags.

To view the list of hosts:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Assets** > **Host Assets**.

   The **Host Assets** page appears.
3. (Optional) To filter the list of hosts, apply a filter. For more information, see Host Asset Filter Components.
4. At the top of the table, click **Export**.

   Tenable Security Center Director exports the host assets in a CSV file.

Host Asset Filter Components

For general information about using filters, see Filters.

Filter Component	Description
Asset Criticality Rating (ACR)	(Requires Tenable Security Center+ license) Filters for hosts within the specified ACR range (for example, between 1 and 5). For more information, see Asset Criticality Rating in the *Tenable One Vulnerability Management User Guide*.

Filter Component	Description
	Tip: To edit the ACR for a host asset, see Edit an ACR Manually.
Address	This filter specifies an IPv4 or IPv6 address, range, or CIDR block to limit the viewed hosts. For example, entering *198.51.100.28/24* and/or *2001:DB8::/32* limits any of the web tools to show only host data from the selected network(s). Addresses can be comma-separated or on separate lines.
Asset Exposure Score (AES)	(Requires Tenable Security Center+ license) Filters for hosts within the specified AES range (for example, between 400 and 600).
DNS Name	This filter specifies a DNS name to limit the viewed hosts. For example, entering host.example.com limits any of the web tools to show only host data from that DNS name.
Name	Filters for hosts with names that include the specified text.
Operating System	Filters for hosts running the specified operating system.
Repositories	Filters for hosts with associated vulnerability data in the specified repository.
System Type	Filters for hosts with the specified device type, as determined by plugin 54615.

Audit Files

The Tenable 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.

For more information on compliance checks and creating custom audits, see the Compliance Checks Reference.

> **Note:** The maximum number of audit files you can include in a single **Policy Compliance Auditing** scan is limited by the total runtime and memory that the audit files require. Exceeding this limit may lead to incomplete or failed scan results. To limit the possible impact, Tenable recommends that audit selection in your scan policies be targeted and specific for the scan's scope and compliance requirements.

Compliance Results in Tenable Security Center

Compliance audit scans are not the same as vulnerability scans, although there can be some overlap. A compliance audit determines whether a system is configured in accordance with an established policy. Compliance check results do not evaluate the risk of non-compliant findings; severity correlations in Tenable Security Center are not a direct indication of threat level or risk. Review compliance check results thoroughly to assess their risk.

Tenable Nessus reports compliance check results as Pass, Warning, or Fail. Tenable Security Center maps these to its standard severity levels as follows:

Tenable Nessus Result	Tenable Security Center Severity
Pass	Info
Warning	Medium
Fail	High

When audit results are imported into Tenable Security Center after a scan completes, compliance audit plugins are assigned plugin numbers from a dedicated range (any value greater than 1,000,000). As a result, compliance plugin numbers may differ between Tenable Security Center instances.

Template-Based Audit Files

You can add template-based audit files using templates embedded within Tenable Security Center Director. Tenable updates these templates regularly through the Tenable Security Center 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 Security Center.

- 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.

Manage Audit Files

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

Add a Template-Based Audit File

You can add template-based audit files using templates embedded within Tenable Security Center Director. Tenable updates these templates regularly through the Tenable Security Center feed.

For more information, see Audit Files.

Note: The maximum number of audit files you can include in a single **Policy Compliance Auditing** scan is limited by the total runtime and memory that the audit files require. Exceeding this limit may lead to incomplete or failed scan results. To limit the possible impact, Tenable recommends that audit selection in your scan policies be targeted and specific for the scan's scope and compliance requirements.

To add a template-based audit file:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Audit Files**.

   The **Audit Files** page appears.
3. Click **Add**

   The **Audit File Templates** page appears.
4. In the **Common** 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 Security Center 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

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 Security Center.

- 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.

> **Note:** The maximum number of audit files you can include in a single **Policy Compliance Auditing** scan is limited by the total runtime and memory that the audit files require. Exceeding this limit may lead to incomplete or failed scan results. To limit the possible impact, Tenable recommends that audit selection in your scan policies be targeted and specific for the scan's scope and compliance requirements.

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 Security Center Director via the user interface.
2. In the left navigation, click **Audit Files**.

   The **Audit Files** page appears.
3. Click **Add**

   The **Audit File Templates** page appears.
4. In the **Other** 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.
9. Click **Submit**.

   Tenable Security Center 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.

View Audit File Details

For more information, see Audit Files.

To view details for an audit file:

1. Log in to Tenable Security Center 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. Click **View**.

   The **View Audit File** page appears.
5. Right-click the row for the audit file.

   The actions menu appears.

   -or-

   Select the check box for the audit file.

   The available actions appear at the top of the table.

Edit or Replace Audit Files

For more information, see Audit Files.

To edit or replace an audit file:

1. Log in to Tenable Security Center 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. Right-click the row for the audit file.

   The actions menu appears.

   -or-

   Select the check box for the audit file.

The available actions appear at the top of the table.

5. Click **Edit**.

   The **Edit Audit File** page appears.

6. To edit the name or description, type a new **Name** or **Description**.
7. To replace the audit file, click the delete button (**x**) next to the file and upload a new audit file.
8. Click **Submit**.

   Tenable Security Center Director saves your configuration.

Share or Revoke Access to Audit Files

For more information, see Audit Files.

To share or revoke access to an audit file:

1. Log in to Tenable Security Center 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. Right-click the row for the audit file.

   The actions menu appears.

   -or-

   Select the check box for the audit file.

   The available actions appear at the top of the table.

5. Click **Share**.
6. Share or revoke access for each group in your organization.
7. Click **Submit**.

   Tenable Security Center Director saves your configuration.

Export Audit Files

For more information, see Audit Files.

To export an audit file:

1. Log in to Tenable Security Center 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. Right-click the row for the audit file.

   The actions menu appears.

   -or-

   Select the check box for the audit file.

   The available actions appear at the top of the table.
5. Click **Export**.

   Tenable Security Center Director exports the audit file.

Delete Audit Files

For more information, see Audit Files.

To delete an audit file:

1. Log in to Tenable Security Center 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. Right-click the row for the audit file.

   The actions menu appears.

   -or-

   Select the check box for the audit file.

   The available actions appear at the top of the table.

5. Click **Delete**.

   A confirmation window appears.

6. Click **Delete**.

   Tenable Security Center 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 on your managed Tenable Security Center instances.

If your deployment includes Tenable Security Center Director, you can use it to manage the scan zones on your managed Tenable Security Center instances.

For more information, see Manage Scan Zones.

Option	Description
Tenable Security Center Director Instance	The name of the managed Tenable Security Center Director instance where you configured the scan zone.
Name	A name for the scan zone.
Description	(Optional) A description for the scan zone.
Ranges	One or more IP addresses that you want the scan zone to target. Supported formats: • a comma-separated list of IP addresses and/or CIDR addresses. • a newline-separated list of IP addresses and/or CIDR addresses.

	• a hyphenated range of IP addresses (e.g., 192.0.2.0-192.0.2.25).
Scanners	One or more scanners that you want to use to scan the **Ranges** in this scan zone. **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**.

Best Practices

Tenable recommends pre-planning your scan zone strategy to efficiently target discrete areas of your network. If configured improperly, scan zones prevent scanners from reaching their targets. Consider the following best practices:

- It is simplest to configure and manage a small number of scan zones with large ranges.
- It is simplest to target ranges (versus large lists of individual IP addresses).
- If you use Tenable Nessus Manager for agent management, do not target Tenable Nessus Manager in any scan zone ranges.
- Tenable Security Center Director fills the least-busy scanner in the zone up to its capacity before moving on to the next. During a scan, you may see one scanner more active than others at any given moment, but the workload evens out across all assigned scanners as the scan progresses.

Selectable Scan Zones

When you configure an active scan, you can select one or more scan zones to determine which scanners run the scan.

Note: If you select a single scan zone, Tenable Security Center Director ignores the IP ranges configured for that scan zone and scans all of the targets you specify in the scan configuration. The scan zone ranges are only used to determine scanner routing when multiple scan zones are selected.

To control which scanners are used based on target IP ranges, select multiple scan zones. Tenable Security Center Director will route targets to the appropriate scanner based on the ranges defined in each zone.

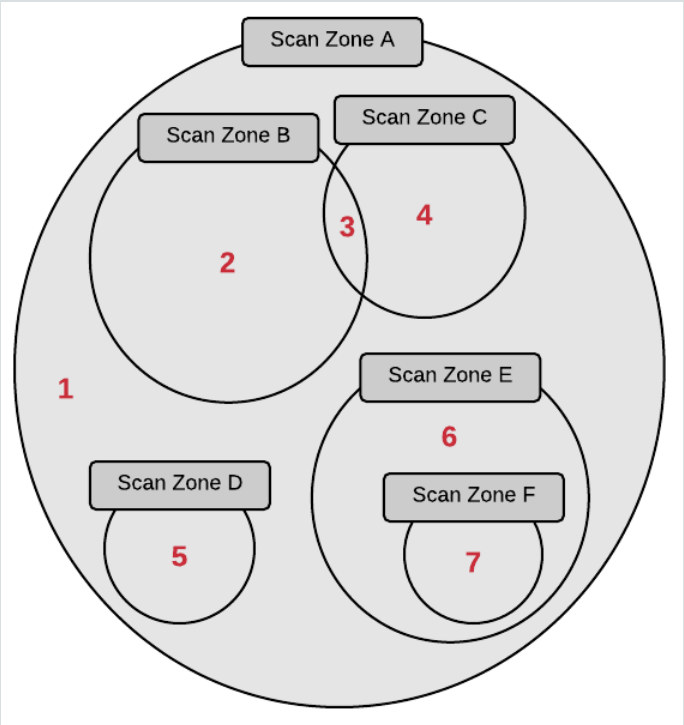
Overlapping Scan Zones

In some cases, you may want to configure overlapping scan zones to ensure scanning coverage or redundancy.

> **Note:** Do not configure overlapping scan zones without pre-planning your scan zone and **Distribution Method** strategy.

Two or more scan zones are redundant if they target the same area of your network. If Tenable Security Center Director executes a scan with redundant scan zones, it first attempts the scan using the narrowest, most specific scan zone.

In this example, the red numbers represent specific IP addresses on your network. The grey circles represent the network coverage of individual scan zones.



See the following table to understand the primary and redundant scan zones for the IP addresses in this example.

IP Address	Primary Scan Zone	Redundant Scan Zones
1	Scan Zone A	None.
2	Scan Zone B	Scan Zone A.
3	Scan Zone C	Scan Zone B, then Scan Zone A.
4	Scan Zone C	Scan Zone A.
5	Scan Zone D	Scan Zone A.
6	Scan Zone E	Scan Zone A.
7	Scan Zone F	Scan Zone E, then Scan Zone A.

Manage Scan Zones

Required Tenable Security Center User Role: Administrator

Add a Scan Zone

You can add a scan zone to a managed Tenable Security Center instance. For more information about scan zone options, see Scan Zones.

To add a scan zone to a managed Tenable Security Center instance:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Scan Infrastructure** > **Scan Zones**.

   The **Scan Zones** page appears.
3. At the top of the table, click **Add**.

The **Add Scan Zone** page appears.

4. In the **Tenable Security Center Instance** drop-down, select the name of the managed Tenable Security Center instance where you want to add the scan zone.

   > **Tip:** If you arrived at the **Add Scan Zone** page from the **Scan Zones** tab on a Tenable Security Center instance details page, you cannot modify the **Tenable Security Center Instance** option.

5. In the **Name** box, type a name for the scan zone.
6. In the **Description** box, type a description for the scan zone.
7. In the **Ranges** box, type one or more IP addresses, CIDR addresses, or ranges to target with the scan zone.
8. In the **Scanners** box, choose one or more scanners to associate with the scan zone.
9. Click **Submit**.

   Tenable Security Center Director saves your configuration.

What to do next:

- Configure scan zone-related organization settings, as described in Organizations.

View Your Scan Zones

For more information, see Scan Zones.

To view a list of configured scan zones:

1. Log in to Tenable Security Center 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 of the scan zone.
   - **Tenable Security Center Instance** – The name of the Tenable Security Center instance where your scan zone is configured. For more information, see Tenable Security Center Director Deployments.

- **Status** – The status of the scan zone.

Scan Zone Status	Description
All Scanners Available	All of the scanners in the scan zone are **Working**.
***x*/*y* Scanners Available**	Only some of the scanners in the scan zone are **Working**.
No Scanners Available	None of the scanners in the scan zone are **Working**.

  For information about **Working** and other scanner statuses, see Tenable Nessus Scanner Statuses.

- **Scanners** – The number of Tenable Nessus scanners in the scan zone.
- **Last Modified** – The date and time the scan zone was last modified.

Edit a Scan Zone

You can modify the options for scan zones on your managed Tenable Security Center instances. For more information about scan zone options, see Scan Zones.

To edit a scan zone on a manged Tenable Security Center instance:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Scan Infrastructure** > **Scan Zones**.

   The **Scan Zones** page appears.
3. Right-click the row for the scan zone you want to edit.

   The actions menu appears.

   -or-

   Select the check box for the scan zone you want to edit.

   The available actions appear at the top of the table.
4. Click **Edit**.

The **Edit Scan Zone** page appears.

5. Modify the following scan zone options. For more information, see Scan Zones.
   - **Name**
   - **Description**
   - **Ranges**
   - **Scanners**

   > **Note:** You cannot move a scan zone from one managed Tenable Security Center instance to another. To change the **Tenable Security Center Instance**, delete the scan zone and add a new scan zone with the same settings on a different Tenable Security Center instance.

6. Click **Submit**.

   Tenable Security Center Director saves your configuration.

Delete a Scan Zone

You can delete a scan zone to permanently remove it from a managed Tenable Security Center instance. For more information, see Scan Zones.

Before you begin:

- Confirm that no scans target the scan zone you want to delete. Tenable Security Center scans may fail if you delete an actively targeted scan zone.

To delete a scan zone:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Scan Infrastructure** > **Scan Zones**.

   The **Scan Zones** page appears.
3. Select the scan zone you want to delete:

- To delete a single scan zone:
    a. In the table, right-click the row for the scan zone you want to delete.

       The actions menu appears.

    b. Click **Delete**.
- To delete multiple scan zones:
    a. In the table, select the check box for each scan zone you want to delete.

       The available actions appear at the top of the table.

    b. At the top of the table, click **Delete**.

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

   Tenable Security Center Director deletes the scan zone from the managed Tenable Security Center instance.

Labels

You can use labels in Tenable Security Center Director to label assets or queries with a custom descriptor to improve filtering and object management. For example, you could add a label named **East Coast Employees** to label all of your assets in that geographic area.

After you create a label and apply it to an object, the label is visible to all users who can view or modify that object. However, label are not shared across object types.

For instructions on creating a new label or adding an existing label, see Add a Label. For instructions on how to delete a label, see Remove or Delete a Label.

Add a Label

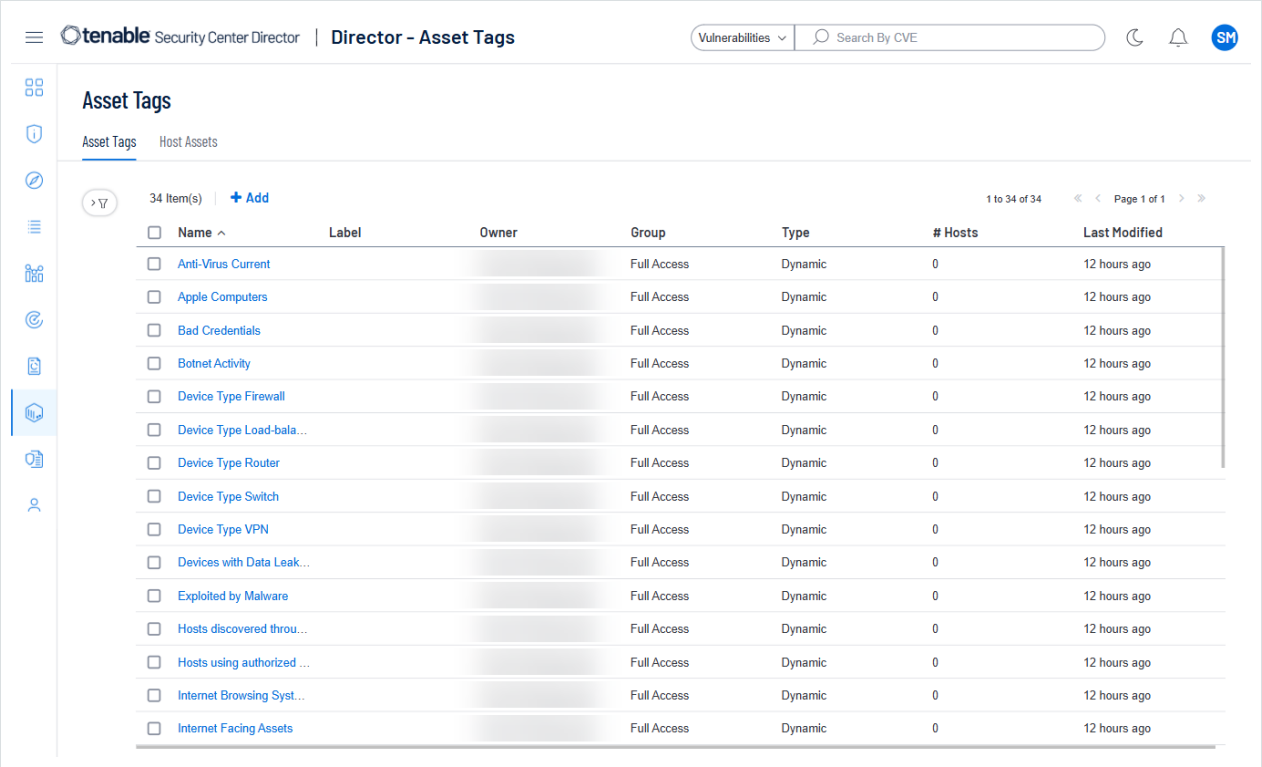
> **Required Tenable Security Center Director User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Labels.

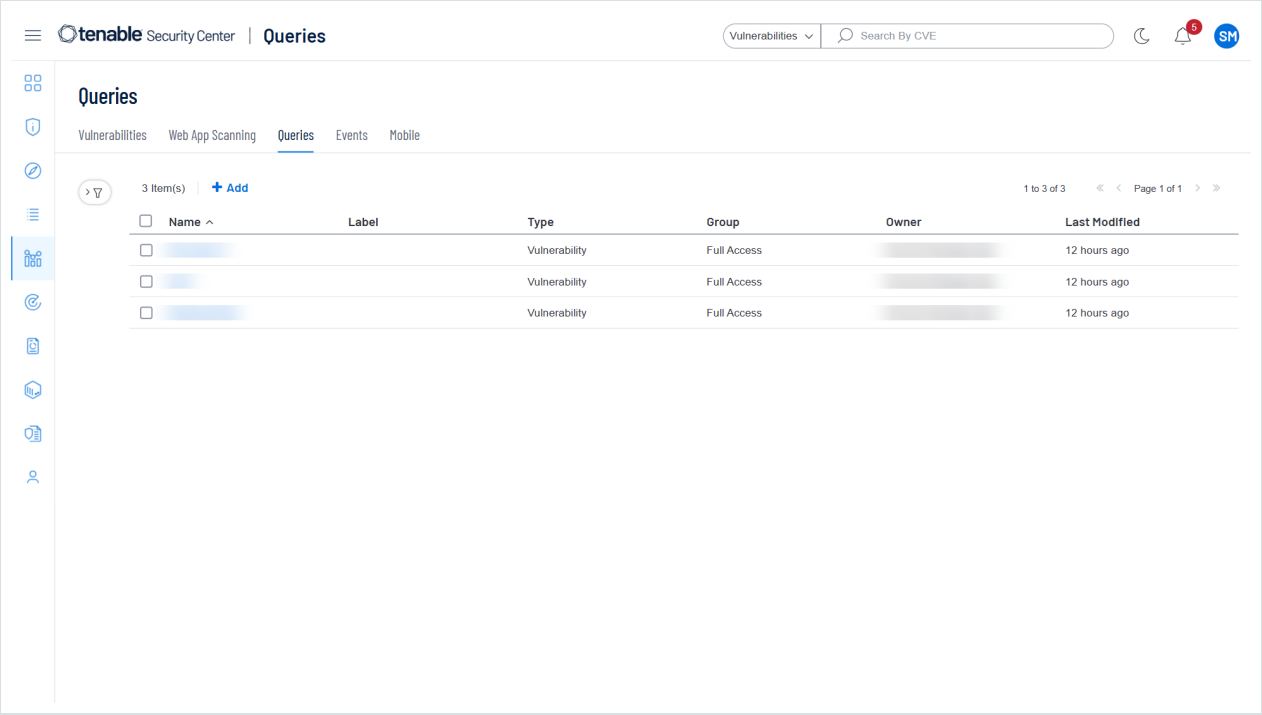
To add a label:

1. Log in to Tenable Security Center Director.
2. Navigate to the assets or queries page:
    - Click **Asset Tags**.

> **Note:** The **Asset Tags** page is available only to Security Manager users.

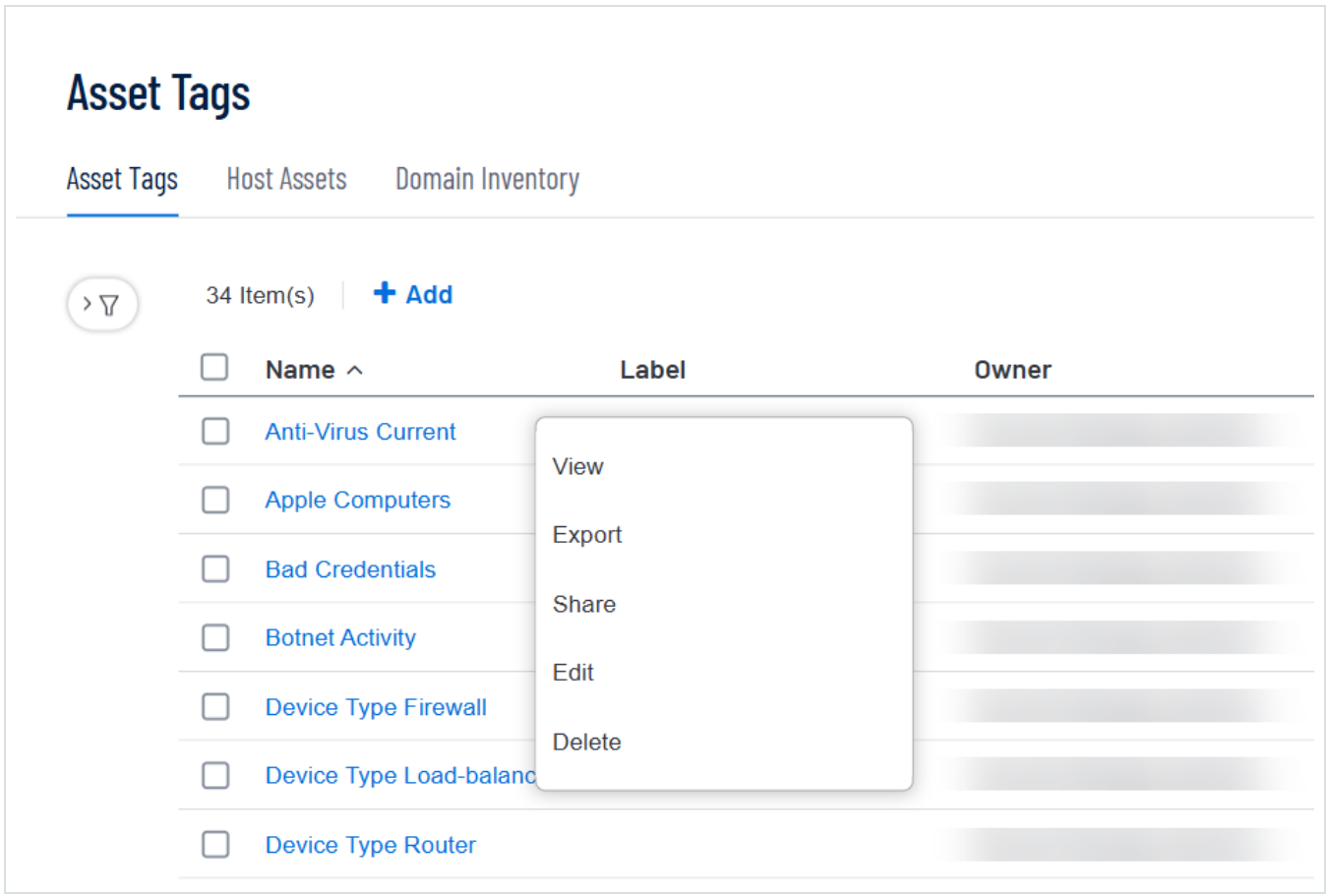


- Click **Analysis** > **Queries**.



3. Right-click the row for the asset or query you want to label.

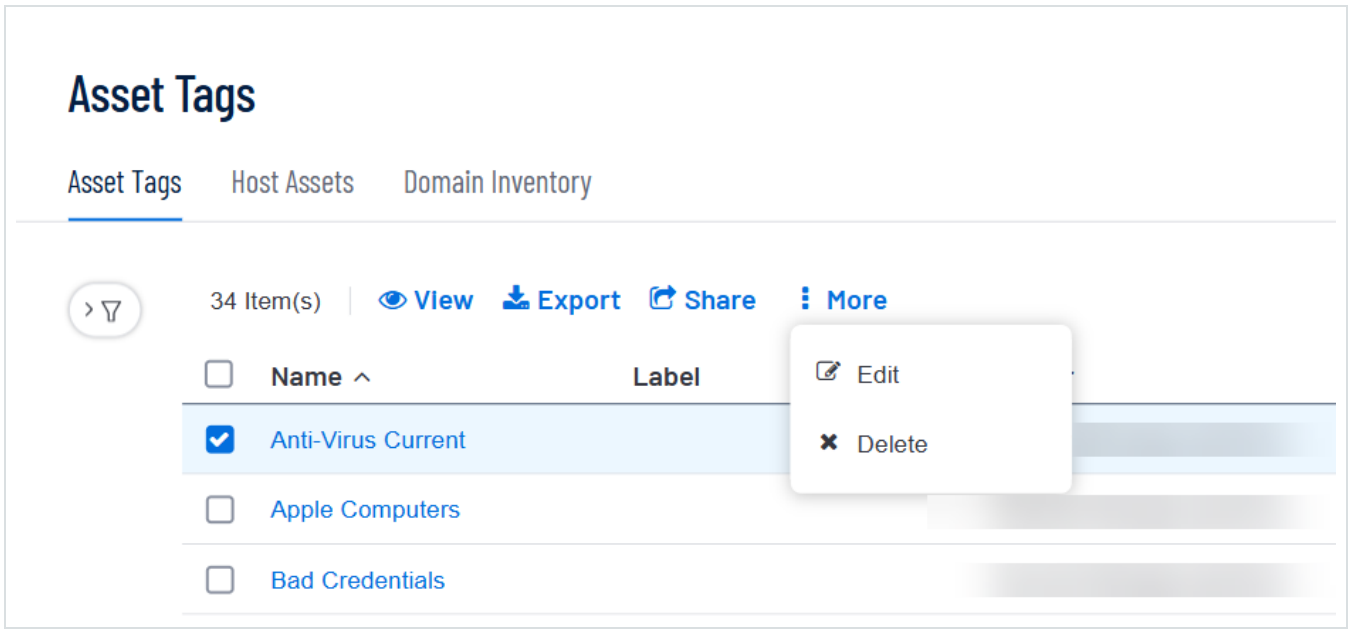
   The actions menu appears.



-or-

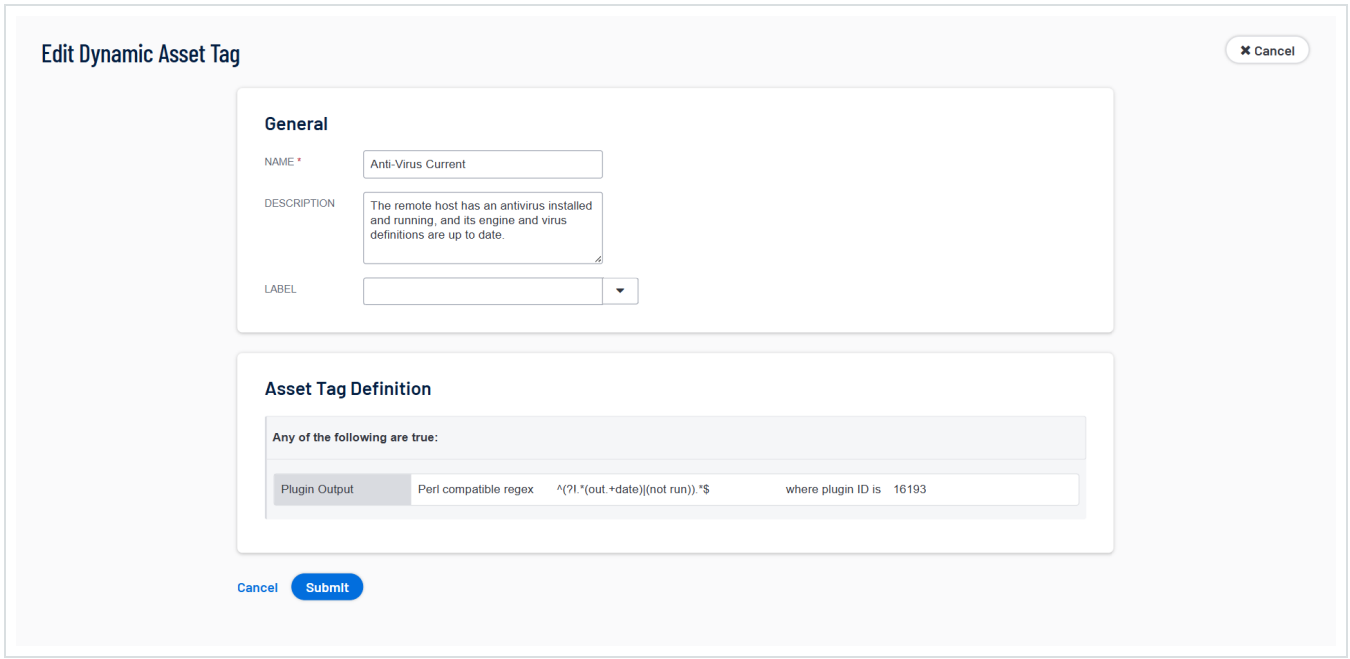
Select the check box for the asset or query you want to label.

The available actions appear at the top of the table.



4. Click **Edit**.

   The **Edit** page appears.



5. In the **Label** drop-down box, select an existing label or type a new label.
6. Click **Submit**.

   The label appears, applied to the asset or query.

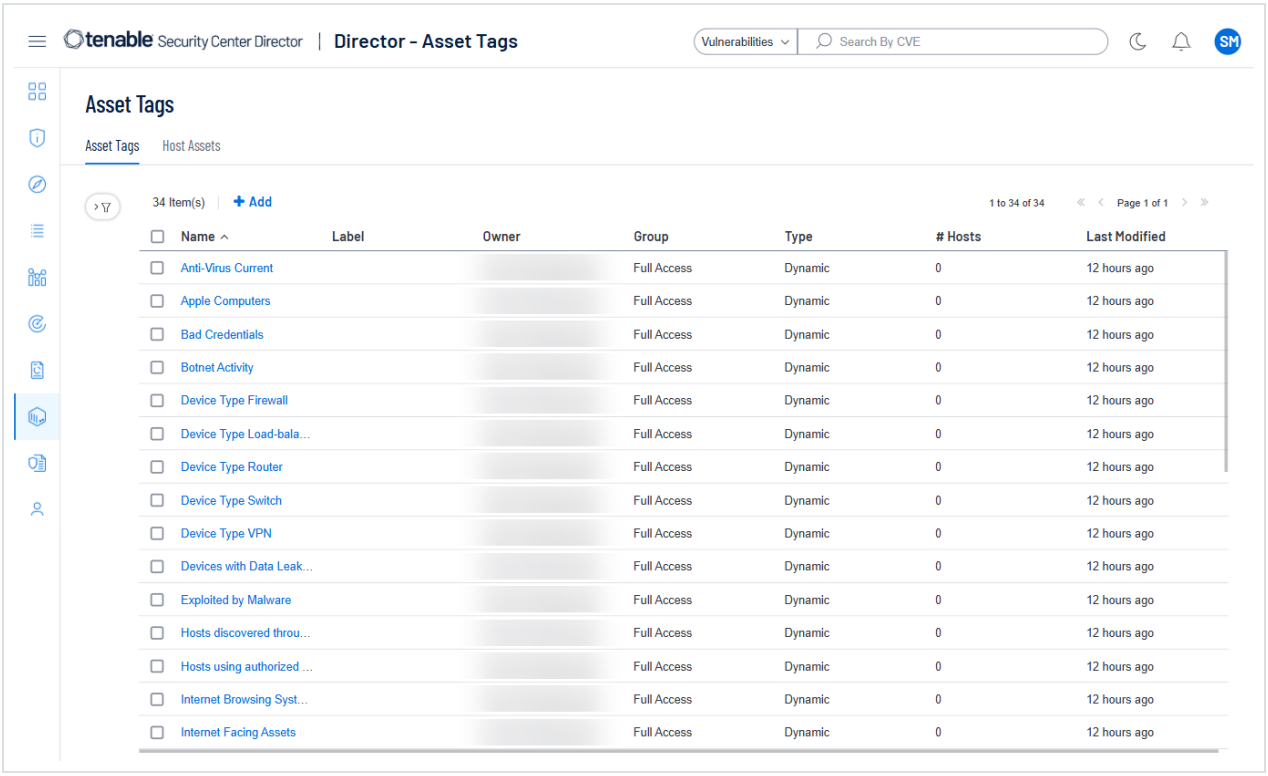
Remove or Delete a Label

Required Tenable Security Center Director User Role: Organizational user with appropriate permissions. For more information, see User Roles.

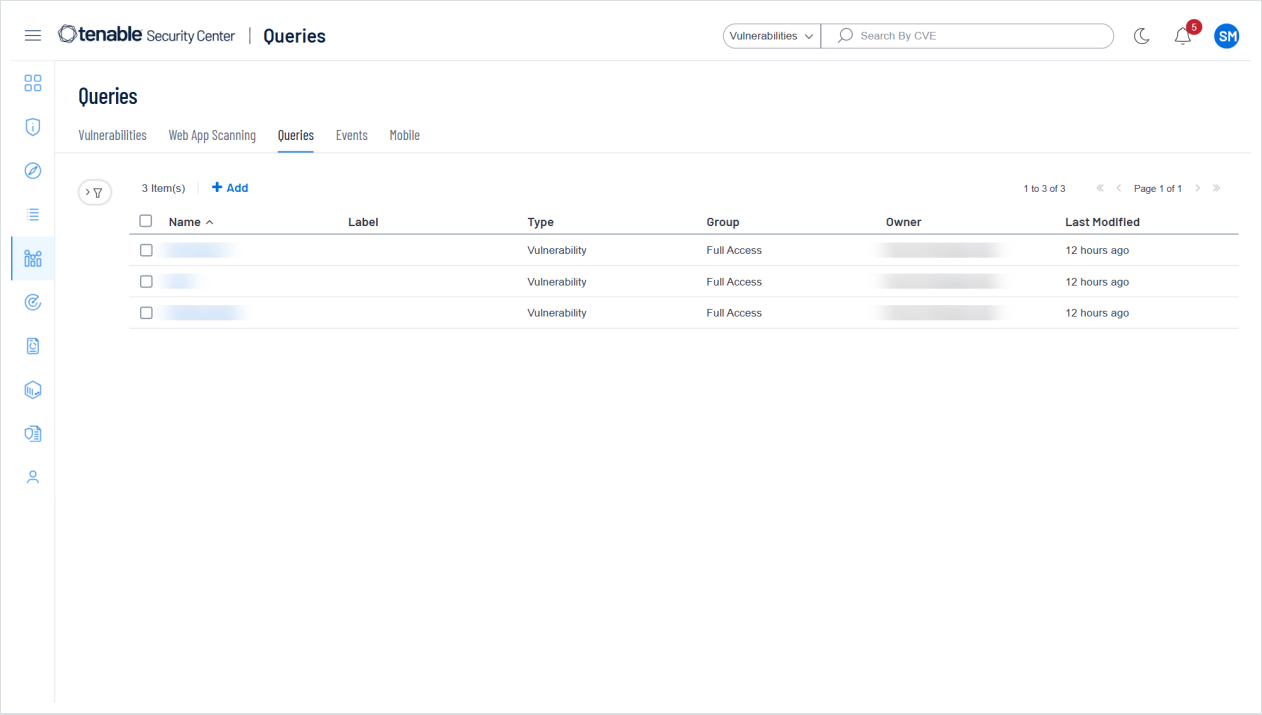
You can remove a label from an asset or query to stop associating that object with the label. To completely delete a label from Tenable Security Center Director, you must remove the label from all assets or queries. For more information, see Labels.

To remove a label or completely delete a label from Tenable Security Center Director:

1. Log in to Tenable Security Center Director via the user interface.
2. Navigate to the **Asset Tags** or **Queries** page:
    - Click **Asset Tags**.

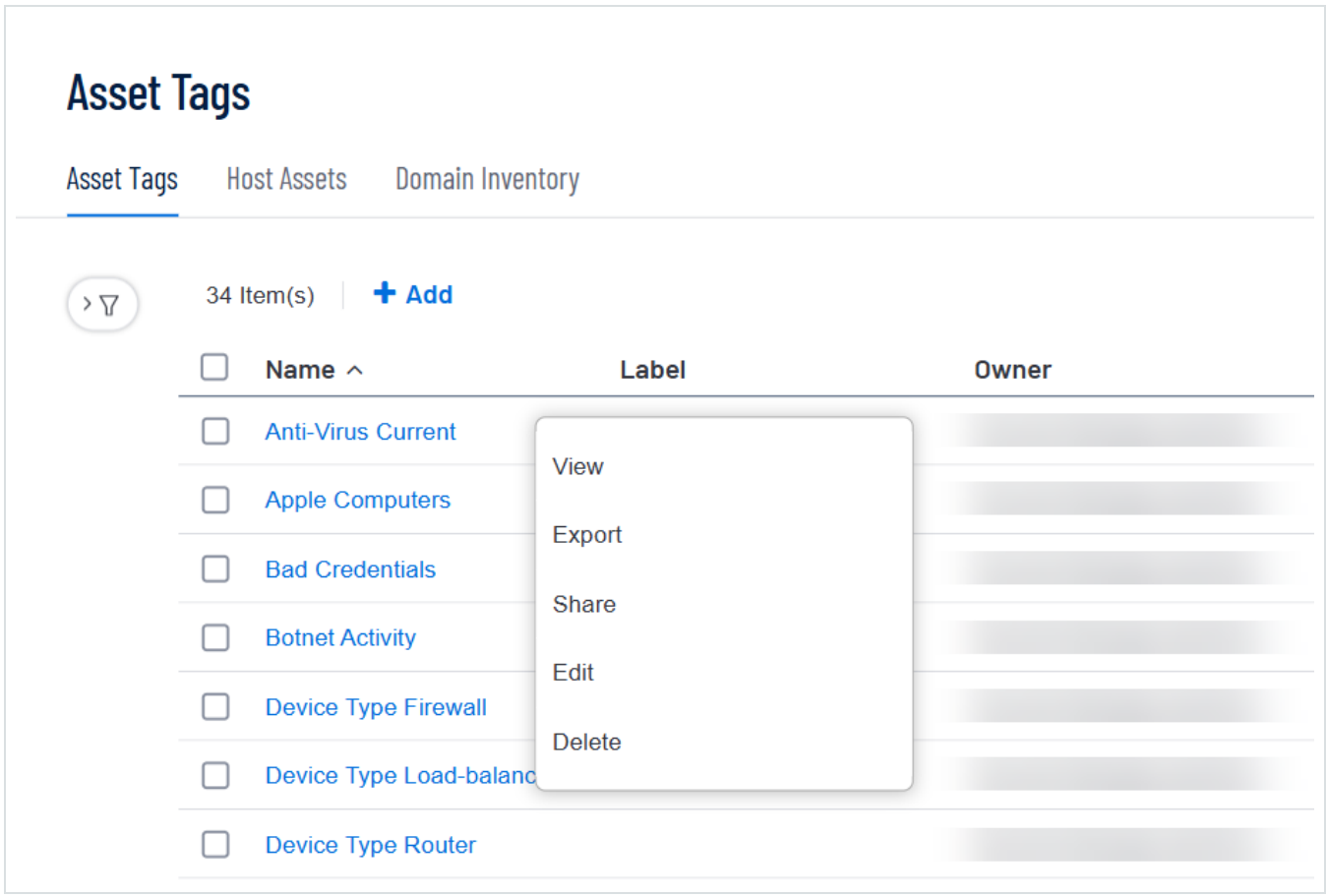


- Click **Analysis** > **Queries**.



3. Right-click the row for the asset or query where you want to remove the label.

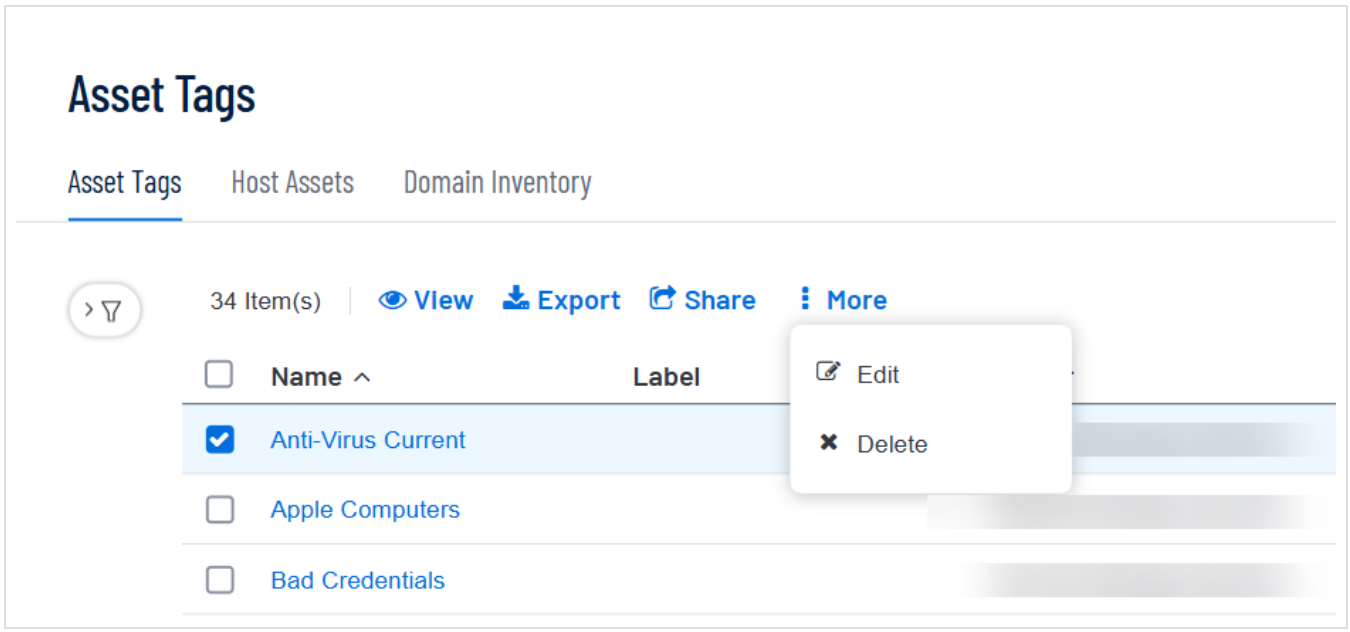
   The actions menu appears.



-or-

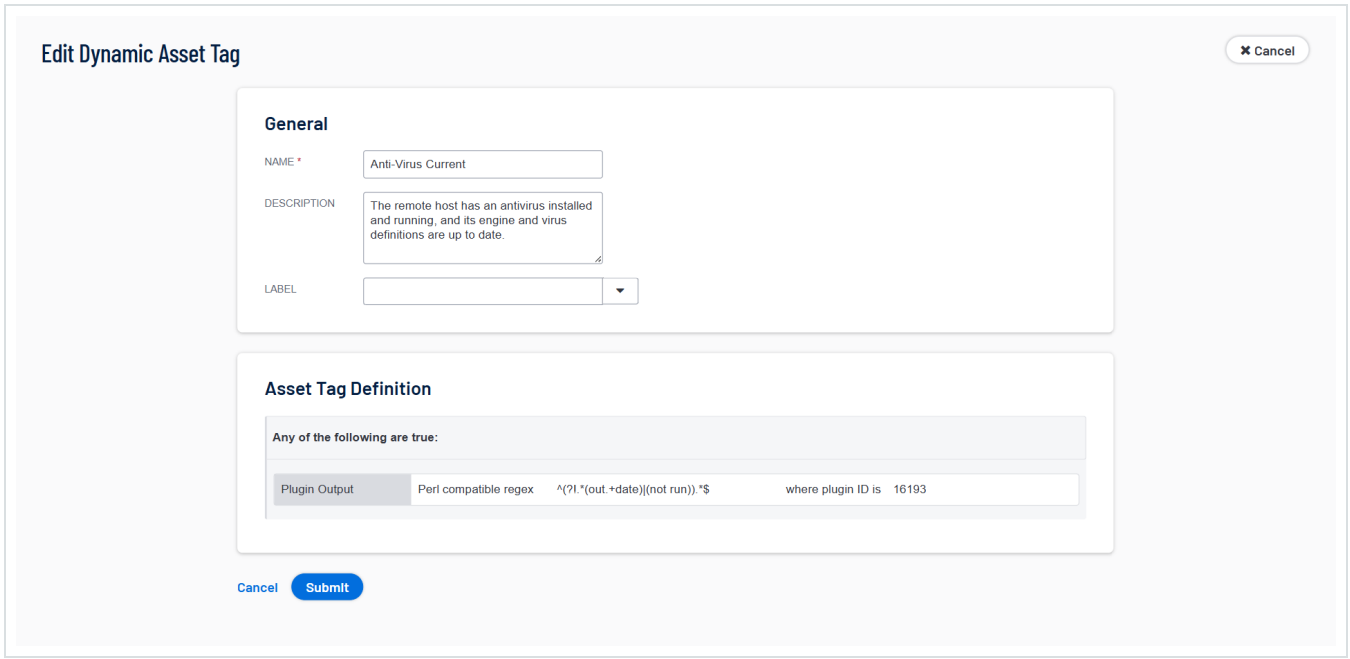
Select the check box for the asset or query where you want to remove the label.

The available actions appear at the top of the table.



4. Click **Edit**.

   The **Edit** page appears.



5. In the **Label** drop-down-box, remove the label from the asset or query.
6. Click **Submit**.

   Tenable Security Center Director removes the label from the asset or query.

7. (Optional) If you want to delete the label from Tenable Security Center Director, repeat steps 2 through 6 until you have removed all uses of the label for the object type.

   Tenable Security Center Director deletes the label.

Analyze Data

Note: To enable cumulative vulnerability data analysis, add the repositories of your managed Tenable Security Center instances as Remote Repositories.

See the following sections to analyze and respond to Tenable Security Center Director data.

Analysis Tool	Description
Scan Results	View a table of scan results from active and agent scans.
Dashboards	View graphical summaries of scans, scan results, and system activity.
Solutions Analysis	View recommended solutions for all vulnerabilities on your network.
Vulnerability Analysis	View a table of cumulative or mitigated vulnerability data.
Reports	Create custom or template-based reports to export Tenable Security Center data for further analysis.

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.

Trending

Trending is a Tenable Security Center Director feature that tracks vulnerability counts over time and displays the results as line and area charts in dashboards and reports. Trending gives you a historical view of how your vulnerability data changes day over day, so you can measure progress toward remediation goals and identify patterns in your security posture.

How Trending Works

When you add a line or area chart component to a dashboard or report, Tenable Security Center Director automatically registers the underlying query with the Trending service. Each day, the Trending service executes all registered queries against your current cumulative vulnerability data and stores the results as a daily data point. Over time, these data points form the trend lines visible in your charts.

Trending uses the `sumseverity` tool for query execution, which aggregates vulnerability counts by severity level (Critical, High, Medium, Low, Info). If a query uses a tool that is not directly supported for trending, Tenable Security Center Director automatically converts it to severity-based aggregation when calculating trend data. The original query tool is preserved for all other uses. A note appears in the UI wherever this conversion applies.

Tenable Security Center Director deduplicates trend execution: if multiple charts reference queries that are logically identical (same filters, organization, and group context), the Trending service executes the query once and shares the results across all matching charts.

Why It's Important

Trending allows you to answer questions that point-in-time vulnerability data cannot: Are we reducing our critical vulnerability count week over week? Did a recent patch cycle have a measurable impact? How does severity distribution shift after a new scan policy is applied?

Without trending, dashboards and reports show only the current state of your environment. With trending, they show the direction and rate of change — information that is essential for demonstrating remediation progress to stakeholders and for identifying regressions quickly.

Requirements and Considerations

New charts start from a single data point. When you create a new trending chart, it begins with one data point representing the current day's vulnerability data. Historical data from before the chart was created is not available. The trend grows by one data point each day as the Trending service runs its scheduled queries.

Editing a chart's query resets its trend data. If you change the query associated with an existing trending chart, the chart resets to a single data point for the current day. Previous trend data for the old query definition is no longer displayed. If you need to preserve existing trend history, avoid modifying the query attached to a trending chart.

Remote repositories must sync at least every 24 hours. If you use remote repositories as data sources for trending charts, configure the remote repository's Update Schedule to sync at least once every 24 hours. Repositories that sync less frequently produce gaps in trending data because the Trending service runs on a daily schedule and requires up-to-date data at execution time. For more information, see Remote Repositories.

Offline repositories may produce gaps in trending data. If you use offline repositories and do not import updated data daily, trending charts that reference that repository's data may have missing data points for days when no import occurred. Tenable recommends reviewing your import schedule if trending accuracy is important for offline repository data.

Trending queries cannot be deleted while in use. If a query is referenced by one or more trending charts in a dashboard or report, you cannot delete the query directly. Remove the query from all trending chart components before deleting it.

For more information, see Dashboards, Reports, and Repositories.

Dashboards

> **Required Tenable Security Center 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, alert, asset, and finding data for analysis. When viewing vulnerability, event, asset, or finding data, you can drill into the underlying

dataset for further evaluation. For more information about displaying asset and finding data from **Explore** in a dashboard component, see Explore Data Source Options.

Tip: Tenable provides many dashboard templates (for example, the VPR Summary dashboard). For a complete index of Tenable-provided dashboard templates, see the Tenable Security Center 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.

Tip: Tenable Security Center automatically refreshes dashboard data once per day. To refresh all dashboard components on demand as an organizational user, click **Refresh All**.

For more information, see:

- View a Dashboard
- Add a Template-Based Dashboard
- Add a Custom Dashboard
- Import a Dashboard
- Manage Dashboards
- Manage Dashboard Components

Dashboard Options

Option	Description
General	

Option	Description
Name	The name of the dashboard.
Description	(Optional) A description for the dashboard.
Layout	The number and arrangement of dashboard columns.

View a Dashboard

Required Tenable Security Center 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 Security Center 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.

    > **Note:** You cannot send a dashboard to a report if it contains a component that uses an **Explore - Assets** or **Explore - Findings** data source. This includes an Explore table, bar chart, or pie chart component; an Explore series in a line or area chart component; and an Explore cell in a matrix component. Reports do not support Explore data sources. For more information, see Explore Data Source Options.
    >
    > If your dashboard contains Explore data, Tenable Security Center Director displays the **Send to Report Unavailable** window, which lists the components, series, or matrix cells that use an Explore data source. A component with no name appears as **Untitled**, an unnamed series appears by position (for example, **Series 2**), and a matrix cell appears by its row and column labels or position (for example, **Row 1, Column 2**). To send the dashboard to a report, remove each listed item or change its data source to a data source other than Explore, and then click **Send to Report** again.
    >
    > If Tenable Security Center Director cannot check the dashboard for Explore data sources (for example, because of a network error), the window instead prompts you to try again.
- Delete the dashboard in view, as described in Delete a Dashboard.
- Customize the table, as described in Interact with a Customizable Table.

Insights Dashboard

Tenable Security Center Director provides the **Insights** dashboard to administrators. For more information, see View a Dashboard.

Widget	Action
Scanners	• View the total number of scanners on all managed Tenable Security

Widget	Action
Connection Status	Center instances and the percentage of scanners that are **Working** or **Not Working**. For more information, see Tenable 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 Tenable Nessus Scanner Statuses.
Scan Zones Status	• View the total number of scan zones on all managed Tenable Security Center instances and the percentage of scan zones that are **Working**, **Degraded**, or **Not Working**. For more information, 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 Security Center **Instance Status**	View the total number of managed Tenable Security Center instances and the percentage of instances that are **Connected** or experiencing a **Connection Error**.

Widget	Action
Tenable Security Center **Instance Plugin Set Age**	View the elapsed time since the last plugin update on your managed Tenable Security Center instances, by plugin age: • **Within 24 Hours** – The number of instances with plugins updated within the last 24 hours. • **1-7 Days Old** – The number of instances with plugins updated between 1 day and 7 days ago. • **8-14 Days Old** – The number of instances with plugins updated between 8 days and 14 days ago. • **Older Than 14 Days** – The number of instances with plugins updated more than 14 days ago.

Scan Results Trend	• View the status of scan results on your managed Tenable Security Center instances, by date, within the selected time frame (last 24 hours or last 7 days). For more information about scan result statuses, see Scan Result Statuses.
	  • **Completed** – The number of scans that completed successfully.
	  • **Partial** – The number of scans that ran, but did not complete.
	  • **Failed** – The number of scans that failed to run.
	• To change the time frame of the scan results shown, click the selectors above the graph:
	  • **24H** – View scan result statuses from the last 24 hours.
	  • **7D** – View scan result statuses from the last 7 days.
	• To show or hide a status in the graph, click the name of the status in the key below the graph.
	• To navigate to a list of **Completed** scan results, click the green section of the graph.

Widget	Action
	• To navigate to a list of **Partial** scan results, click the orange section of the graph. • To navigate to a list of **Failed** scan results, click the red section of the graph.

Scanning Overview	• View a list of all scans that are **Running** or **Paused** on your managed Tenable Security Center instances, by Tenable Security Center instance name and scan name. Scans with a purple bar are **Running** and scans with a grey bar are **Paused**.
	• Hover over the timeline for a scan to view additional details:
	  • **Tenable Security Center Instance** – The name of the managed Tenable Security Center instance where the scan is running.
	  • **Progress** – The number of scanned hosts compared to the total number of hosts to scan.
	  • **Started** – The date and time the scan started.
	  • **Estimated Remaining Time** – The estimated time to scan completion.

Licensing Status	View a graph showing the total number of assets counting toward your license compared to your total license size. For more information about Tenable Security Center licenses, see License Requirements.

Set a Dashboard as Your Default Dashboard

Required Tenable Security Center 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 Security Center 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.

Add a Template-Based Dashboard

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can add a dashboard by configuring a Tenable-provided dashboard template. To add a custom dashboard instead, see Add a Custom Dashboard. To import a dashboard, see Import a Dashboard.

For more information, see Dashboards and Dashboard and Component Templates.

To add a template-based dashboard:

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, 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 **Dashboard Templates** page appears.
5. In the **Common** 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.
   - To edit the dashboard refresh schedule, click the **Schedule** link.
8. Click **Add**.

   Tenable Security Center Director 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 Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can add a fully customized dashboard. To add a dashboard from a Tenable-provided template instead, see Add a Template-Based Dashboard.

For more information, see Dashboards.

To add a custom dashboard:

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, 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 **Dashboard Templates** page appears.
5. In the **Other** 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 Security Center Director 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.

Dashboard and Component Templates

Tenable Security Center provides a selection of dashboards and dashboard component templates. You can configure a Tenable-provided dashboard template or you can create a fully customized dashboard. For more information, see Dashboards and Custom Dashboard Component Options.

For a complete index of Tenable-provided report templates, see the Tenable Security Center Dashboards blog.

Template	Description
Common	
Compliance & Configuration Assessment	Dashboards that aid with configuration, change, and compliance management.
Discovery & Detection	Dashboards that aid in trust identification, rogue detection, and new device discovery.
Executive	Dashboards that provide operational insight and metrics geared towards executives.
Monitoring	Dashboards that provide intrusion monitoring, alerting, and analysis.
Security Industry Trends	Dashboards related to trends, reports, and analysis from industry leaders.
Threat Detection & Vulnerability Assessments	Dashboards that aid with identifying vulnerabilities and potential threats.
Other (Dashboards)	
Advanced	A custom dashboard with no pre-configured settings.
Import	Import a dashboard. For more information, see Import a Dashboard.
Other (Dashboard Components)	
Table	Add a table to your dashboard.
Bar Chart	Add a bar chart to your dashboard.
Pie Chart	Add a pie chart to your dashboard.

Matrix	Add a matrix to your dashboard.
Line Chart	Add a line chart to your dashboard.
Area Chart	Add an area chart to your dashboard.

Import a Dashboard

Required Tenable Security Center 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 Security Center 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 **Dashboard Templates** page appears.
5. In the **Other** section, click **Import**.

   The **Import Dashboard** page appears.
6. In the **Name** box, type a name for the dashboard.
7. Click **Choose File** and browse to the dashboard file you want to import.
8. Click **Submit**.

   Tenable Security Center Director imports the dashboard.

Manage Dashboards

Required Tenable Security Center 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 Security Center 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, right-click the dashboard.

   -or-

   To manage multiple dashboards, select the check box for the dashboard.

   The actions menu appears.

   From this menu, you can:

   - Click **View** to view details for the dashboard.
   - Click **Share** to share or revoke access to the dashboard.
   - Click **Export** to download an XML version of the dashboard.
   - Click **Copy** to copy the dashboard.
   - Click **Edit** to edit the dashboard.
   - Click **Hide from Dashboard** to hide the dashboard from the **Switch Dashboard** drop-down on the **Dashboards** page.

- Click **Show on Dashboard** to show the dashboard on the **Switch Dashboard** drop-down on the **Dashboards** page.
- Click **Delete** to delete the dashboard.

8. To export the dashboard as an XML file:
    a. Click **Export**.
    b. Then, identify how you want Tenable Security Center 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 Security Center Director versions.

Share or Revoke Access to a Dashboard

> **Required Tenable Security Center 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 Security Center 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 Security Center Director saves your configuration.

Delete a Dashboard

> **Required Tenable Security Center 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 Security Center 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 **Delete**.

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

   The system deletes the dashboard.

Manage Dashboard Components

> **Required Tenable Security Center 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 Security Center Director via the user interface.
2. Click **Dashboard**.

   The **Dashboards** page appears.
3. To edit a dashboard component:
   a. Hover over the dashboard component.
   b. Click the ••• menu.

      The actions menu appears.
   c. Click **Edit**.
   d. Edit the dashboard component options. For more information, see Custom Dashboard Component Options.
4. To view the data behind a dashboard component:
   a. Hover over the dashboard component.
   b. In the lower right corner, click **View Data**.

The analysis page appears. If the component uses an **Explore - Assets** or **Explore - Findings** data source, the corresponding **Explore** page appears in the same browser tab, with the component's filters and grouping applied.

> **Note:** Only dashboard components that display vulnerability analysis, event analysis, or **Explore** data support viewing the data behind a dashboard component. **View Data** is not available for the following components:
>
> - Matrix, line chart, and area chart components.
> - Explore components that you group by **Network**.
> - Components that have errors.

5. To view the **Explore** data behind a bar or pie chart component:
   a. Click a bar, a pie chart slice, or a pie chart legend item.

      The **Explore - Assets** or **Explore - Findings** page appears in the same browser tab, filtered to the group that you clicked. For example, if you click the bar for a single CVE, **Explore** filters the page to that CVE ID.

      > **Note:** You cannot click a bar or slice if you group the component by **ACR Severity**, **Asset Tag**, or **Network**. You also cannot click the **Other** slice of a pie chart. Matrix cells that use an **Explore** data source do not open **Explore**.

6. To reorder a dashboard component:
   a. Click the title of a dashboard component.
   b. Drag the dashboard component around the page.
7. To copy a dashboard component to the dashboard in view or a different dashboard:
   a. Hover over the dashboard component.
   b. Click the ••• menu.

      The actions menu appears.

   c. Click **Copy**.
   d. In the **Name** box, edit the name for the copied dashboard component.

e. In the **Dashboard** drop-down box, click the name of the dashboard where you want to copy the dashboard component.

f. Click **Copy**.

Tenable Security Center Director copies the dashboard component.

8. To refresh the dashboard component data:

a. Hover over the dashboard component.

b. Click the ••• menu.

The actions menu appears.

c. Click **Refresh**.

Tenable Security Center Directorrefreshes the dashboard component data.

9. To delete the dashboard component:

a. Hover over the dashboard component.

b. Click the ••• menu.

The actions menu appears.

c. Click **Delete**.

A confirmation window appears.

d. Click **Delete**.

Tenable Security Center Director deletes the dashboard component.

Add a Template-Based Dashboard Component

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can add a dashboard component by configuring a Tenable-provided dashboard component template. To add a custom dashboard component instead, see Add a Custom Dashboard Component.

For more information, see Dashboards and Dashboard and Component Templates.

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 Security Center Director 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 **Component Templates** page appears.
7. In the **Common** section, 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** drop-down box.
   - To edit the dashboard component refresh schedule, click the **Schedule** link.
9. Click **Add**.

   Tenable Security Center Director saves your configuration and the **Dashboards** page appears.

Add a Custom Dashboard Component

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

You can configure a custom dashboard component to add a table, bar chart, pie chart, line chart, area chart, or matrix to a dashboard. For more information, see Dashboards and Dashboard and Component Templates.

For an example matrix component configuration, see Configure a Simple Matrix Dashboard Component.

Table, bar chart, pie chart, matrix, and line and area chart components can also display asset and finding data from **Explore**. For more information, see Explore Data Source Options.

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 Security Center Director via the user interface.
2. In the left navigation, 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 page appears.
5. In the upper-right corner of the page, click the **Options** drop-down box.
6. Click **Add Component**.

   The **Component Templates** page appears.
7. In the **Other** section, click the type of component you want to configure.

   The component configuration page appears.

8. Configure the options for your component type, as described in Custom Dashboard Component Options.
9. Click **Submit**.

   Tenable Security Center Director saves your configuration.

Custom Dashboard Component Options

Use the following options to configure custom dashboard components. For more information about dashboard component types, see Dashboard and Component Templates.

Tenable Security Center supports the following custom dashboard components:

- Table Component Options
- Bar Chart Component Options
- Pie Chart Component Options
- Matrix Component Options
- Line and Area Chart Component Options

Table, bar chart, pie chart, matrix, and line and area chart components can also use asset and finding data from **Explore** instead of the analysis tools. For more information, see Explore Data Source Options.

General Options

Configure the following options for all custom dashboard component types.

Option	Description	Default
Name	(Required) A name for the dashboard component.	--
Description	A description for the dashboard component. The description appears on the **Dashboards** page when you hover over a dashboard component.	--

Option	Description	Default
Schedule	(Required for all except **Matrix** components) Specifies how often the component polls the data source to obtain updates: • **Never** – The component never polls the data source. • **Minutely** – Polls every 15, 20, or 30 minutes. • **Hourly** – Polls every 1, 2, 4, 6, or 12 hours. • **Daily** – Polls daily or every specified number of days at the specified time. • **Weekly** – Polls weekly or every specified number of weeks at the specified time. • **Monthly** – Polls monthly or every specified number of months at the specified day and time. **Caution:** Excessively frequent updates may cause the application to become less responsive due to the added processing load imposed on the host OS.	Daily

Explore Data Source Options

In addition to the analysis tools, you can configure a dashboard component to display asset or finding data from **Explore**. To use an **Explore** data source, select **Explore - Assets** or **Explore - Findings** as the **Type** (or **Data Type**) option.

Note: Explore - Findings is a preview feature. Some functionality may change before general availability.

Availability

The following table shows which components support each **Explore** data source.

Component	Field	Explore - Assets	Explore - Findings
Table	Type	Yes	Yes
Bar chart	Type	Yes	Yes
Pie chart	Type	Yes	Yes
Matrix (each cell)	Data Type	Yes	Yes
Line and area chart (each series)	Data Type	--	Yes (**Severity** grouping only)

Component Options

When you select an **Explore** data source, the component form changes:

- The **Query**, **Source**, and **Tool** options do not appear.
- A **Group By** option and the **Filters** query builder appear below the **Type** option.

For information about the remaining options, see the options table for each component type.

Group By

The **Group By** option determines how the component groups the data. The available options depend on the data source.

Group By	Explore - Assets	Explore - Findings	Notes
None	Yes	Yes	No grouping. The data source returns one row per asset or finding. Available in table and matrix components only, where it is the

Group By	Explore - Assets	Explore - Findings	Notes
			default.
ACR Severity	Yes	--	(Requires Tenable Security Center+ license)
Asset	--	Yes	
Asset Tag	Yes	Yes	
CVE	Yes	Yes	
IAVM	Yes	Yes	
Microsoft ID	Yes	--	
Network	Yes	--	When you select **Network**, a second drop-down box appears next to **Group By** where you select the network class: **Class A** (default), **Class B**, or **Class C**.
Operating System	Yes	Yes	
Severity	--	Yes	The only option for line and area chart series.
System Type	Yes	--	
Vulnerability	Yes	Yes	Groups the data by plugin (plugin ID and plugin name).

The default **Group By** option depends on the component:

- Table and matrix components: **None**.
- Bar chart and pie chart components: the first option in the list, because these charts require a grouping. For **Explore - Assets**, this is **ACR Severity** (or **Asset Tag** if you do not have a Tenable Security Center+ license). For **Explore - Findings**, this is **Asset**.
- Line and area chart series: **Severity**.

For more information about the groupings, see Explore Assets and Using Group By Options on the Findings Page.

Filters

The **Filters** option is the same query builder that you use on the **Explore** pages. It supports the same operators (including NOT groups and wildcard operators such as contains, starts with, and ends with) and the same license requirements. For information about the available filters, see Asset Filters and Findings Filters.

- The **Asset Tag** and **Repository** filters are not available in dashboard components for either data source. The **Plugin Family** filter is also not available for **Explore - Findings**.
- If you do not define any filters, the component uses all of the data from the data source.
- If a filter is incomplete or invalid, Tenable Security Center Director highlights it and you cannot save the component until you correct it.
- If you change the **Type** between **Explore - Assets** and **Explore - Findings**, Tenable Security Center Director clears the filters.

Limitations

- **Explore - Findings** components always use cumulative findings. You cannot chart mitigated findings from **Explore**.
- **Explore** data sources are available in dashboard components only. They are not available in report elements, on the **Add Query** page, or in alerts, tickets, or Assurance Report Cards. You cannot send a dashboard that contains an **Explore** component to a report. For more

information, see View a Dashboard.

- Matrix cells that use an **Explore** data source do not open **Explore** when you click them.

Table Component Options

Option	Description	Default
Data		
Type	The type of data: **Vulnerability**, **Event**, **Mobile**, **User**, **Ticket**, **Alert**, **Explore - Assets**, or **Explore - Findings**. For more information about Explore data sources, see Explore Data Source Options.	Vulnerability
Query	(Not available if **Type** is **Explore - Assets** or **Explore - Findings**.) 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.	--
Source	(If **Type** is **Vulnerability** or **Event**) Specifies the data source. For vulnerability data, select **Cumulative** or **Mitigated**. For event data, the data source is **Active**. Tenable Security Center can use only active event data for event-based components.	Cumulative
Tool	(Not available if **Type** is **Explore - Assets** or **Explore - Findings**.)	Vulnerability Summary

Option	Description	Default
	The analysis tool to use for creating the chart. For more information, see Vulnerability Analysis Tools and Event Analysis Tools.	
Group By	(If **Type** is **Explore - Assets** or **Explore - Findings**) How the data is grouped. • **Explore - Assets**: **None**, **ACR Severity**, **Asset Tag**, **CVE**, **IAVM**, **Microsoft ID**, **Network**, **Operating System**, **System Type**, or **Vulnerability** • **Explore - Findings**: **None**, **Asset**, **Asset Tag**, **CVE**, **IAVM**, **Operating System**, **Severity**, or **Vulnerability** For more information, see Explore Data Source Options.	None
Filters	Additional filters to use on the data source. For more information, see Filters. (If **Type** is **Explore - Assets** or **Explore - Findings**) Use the **Explore** query builder to define the filters that select the data to display. For more information, see Explore Data Source Options.	--
Display		
Results Displayed	The number of displayed results. You can choose to display up to 999 results.	10

Option	Description	Default
	If the **Viewport Size** setting is smaller than this setting, the results display is limited to the **Viewport Size** setting with a scrollbar to display the additional results.	
Viewport Size	The number of records (maximum: 50) to display along with a scrollbar to handle additional records. For example, if **Results Displayed** is set to **100** and **Viewport Size** is **15**, 15 records are displayed with a scrollbar to view the additional 85 records.	10
Sort Column	(Not available if **Type** is **Event**) The column Tenable Security Center uses to sort the results.	Plugin ID (If **Type** is **Explore - Assets** or **Explore - Findings**) The first column for the selected **Group By**.
Sort Direction	(Not available if **Type** is **Event**) The sort direction: **Descending** or **Ascending**.	Descending
Display Columns	The columns to display in the component output. (If **Type** is **Explore - Assets** or **Explore - Findings**) The available columns depend on the selected **Group By**. All columns for the selected **Group By** are selected by default.	--

Bar Chart Component Options

Option	Description	Default
Data		
Type	The type of data: **Vulnerability**, **Event**, **Mobile**, **Ticket**, **Explore - Assets**, or **Explore - Findings**. For more information about Explore data sources, see Explore Data Source Options.	Vulnerability
Query	(Not available if **Type** is **Explore - Assets** or **Explore - Findings**.) 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.	--
Source	(If **Type** is **Vulnerability** or **Event**) Specifies the data source. For vulnerability data, select **Cumulative** or **Mitigated**. For event data, the data source is **Active**. Tenable Security Center can use only active event data for event-based components.	Cumulative
Tool	(Not available if **Type** is **Explore - Assets** or **Explore - Findings**.) The analysis tool to use for creating the chart. For more information, see Vulnerability Analysis Tools and Event Analysis Tools.	Vulnerability Summary

Option	Description	Default
Group By	(If **Type** is **Explore - Assets** or **Explore - Findings**) How the data is grouped. • **Explore - Assets**: **ACR Severity**, **Asset Tag**, **CVE**, **IAVM**, **Microsoft ID**, **Network**, **Operating System**, **System Type**, or **Vulnerability** • **Explore - Findings**: **Asset**, **Asset Tag**, **CVE**, **IAVM**, **Operating System**, **Severity**, or **Vulnerability** For more information, see Explore Data Source Options. The default is the first option in the list for the selected **Type**.	First option in list
Filters	Additional filters to use on the data source. For more information, see Filters. (If **Type** is **Explore - Assets** or **Explore - Findings**) Use the **Explore** query builder to define the filters that select the data to display. For more information, see Explore Data Source Options.	--
Display		
Results Displayed	The number of displayed results. You can choose to display up to 100 results.	10
Sort Column	(If **Type** is **Vulnerability**, **Ticket**, **Explore - Assets**,	Plugin ID

Option	Description	Default
	or **Explore - Findings**) The column Tenable Security Center uses to sort the results.	(If **Type** is **Explore - Assets** or **Explore - Findings**) The first column for the selected **Group By**, which is usually the group name rather than a count.
Sort Direction	(If **Type** is **Vulnerability**, **Ticket**, **Explore - Assets**, or **Explore - Findings**) The sort direction: **Descending** or **Ascending**.	Descending
Display Column	The columns to display in the component output. (If **Type** is **Explore - Assets** or **Explore - Findings**) Only numeric columns are available. By default, all of them are selected, and each selected column appears as its own set of bars. For example, if you group by **CVE**, the chart plots VPR, EPSS, CVSSv4, CVSSv3, CVSSv2, and the total count as separate series.	--

Tip: To create a bar chart that shows the top results by count for an **Explore** data source, set **Sort Column** to **Total** (**Explore - Assets**) or **Vuln Count** (**Explore - Findings**), set **Sort Direction** to **Descending**, and select only that column in **Display Column**.

Pie Chart Component Options

Option	Description	Default
Data		
Type	The type of data: **Vulnerability**, **Event**, **Mobile**, **Ticket**, **Explore - Assets**, or **Explore - Findings**. For more information about Explore data sources, see Explore Data Source Options.	Vulnerability
Query	(Not available if **Type** is **Explore - Assets** or **Explore - Findings**.) 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.	--
Source	(If **Type** is **Vulnerability** or **Event**) Specifies the data source. For vulnerability data, select **Cumulative** or **Mitigated**. For event data, the data source is **Active**. Tenable Security Center can use only active event data for event-based components.	Cumulative
Tool	(Not available if **Type** is **Explore - Assets** or **Explore - Findings**.) The analysis tool to use for creating the chart. For more information, see Vulnerability Analysis Tools and Event Analysis Tools.	Vulnerability Summary

Option	Description	Default
Group By	(If **Type** is **Explore - Assets** or **Explore - Findings**) How the data is grouped. • **Explore - Assets**: **ACR Severity**, **Asset Tag**, **CVE**, **IAVM**, **Microsoft ID**, **Network**, **Operating System**, **System Type**, or **Vulnerability** • **Explore - Findings**: **Asset**, **Asset Tag**, **CVE**, **IAVM**, **Operating System**, **Severity**, or **Vulnerability** For more information, see Explore Data Source Options. The default is the first option in the list for the selected **Type**.	First option in list
Filters	Additional filters to use on the data source. For more information, see Filters. (If **Type** is **Explore - Assets** or **Explore - Findings**) Use the **Explore** query builder to define the filters that select the data to display. For more information, see Explore Data Source Options.	--
Display		
Results Displayed	The number of displayed results.	10
Sort Column	The column Tenable Security Center uses to sort the results.	Plugin ID (If **Type** is **Explore -**

Option	Description	Default
		Assets or **Explore - Findings**) The first column for the selected **Group By**.
Sort Direction	The sort direction: **Descending** or **Ascending**.	Descending
Display Column	The columns to display in the component output. (If **Type** is **Explore - Assets** or **Explore - Findings**) A single count column. The default is **Total** for **Explore - Assets** and **Vuln Count** for **Explore - Findings**. For some groupings, the chart includes an **Other** slice.	--

Matrix Component Options

For information about configuring matrix components and to download samples, visit the Tenable Security Center Dashboards blog. For an example matrix component, see Configure a Simple Matrix Dashboard Component.

When you create a matrix component, you define rules to determine what displays in each cell in a table of customizable columns and rows.

- Use columns to define a group of vulnerability, mobile, event, ticket, user, alert, asset, or finding data. For example, you could create columns for critical, high, medium, low, and informational vulnerabilities.
- Use rows to define the operations performed against each column element for that row. For example, if each column determines the vulnerability type (critical, high, medium, low, and informational), you can create a row to calculate the ratio of the particular vulnerability type count against the total vulnerability count.

By default, each cell definition includes a single customizable rule that defines what appears in the cell if no other conditions have been defined or triggered.

Tenable Security Center reviews each rule in a cell from top to bottom and triggers the display rule on the first rule match. Once a rule triggers, Tenable Security Center stops reviewing rules for the cell. If none of the added rules match, Tenable Security Center performs the default rule.

Option	Action
Cells	
Size	Use the drop-down menus to select the number of columns and rows for the matrix. Tenable Security Center supports matrices from 1x1 to 10x10. Click **Generate Cells** create a blank matrix with customizable cells.
••• icon	Click the ••• icon in a row or column header cell to manage the column or row. • To edit the header name or refresh frequency, click **Edit Header**. **Tip:** You can choose to refresh the data more often to see the most current view. However, frequent refreshes can cause slow system performance. • To delete the row or column, click **Delete Cells**. Tenable Security Center deletes the row or column. • To copy the row or column, click **Copy**. Tenable Security Center copies the row or column.
✎ icon	Click the ✎ icon inside a cell to configure rules for the cell. For more information, see Matrix Component Query Options.

Matrix Component Query Options

Option	Description	Default
Data		
Data Type	The type of data: **Vulnerability**, **Mobile**, **Event**, **User**, **Alert**, **Ticket**, **Explore - Assets**, or **Explore - Findings**. For more information about Explore data sources, see Explore Data Source Options. The **Data Type** determines which query values are available in the **Condition** option.	Vulnerability
Type	The matrix component display type: **Count** or **Ratio**	Count
Source	(If **Data Type** is **Vulnerability** or **Event**) Specifies the data source. For vulnerability data, select **Cumulative** or **Mitigated**. For event data, the data source is **Active**. Tenable Security Center can use only active event data for event-based components.	Cumulative
Group By	(If **Type** is **Count** and **Data Type** is **Explore - Assets** or **Explore - Findings**) How the data is grouped. For the available options, see Explore Data Source Options.	None
Numerator Group By	(If **Type** is **Ratio** and **Data Type** is **Explore - Assets** or **Explore - Findings**) How the numerator data is grouped. For the available options, see Explore Data Source Options.	None
Denominator Group By	(If **Type** is **Ratio** and **Data Type** is **Explore - Assets** or **Explore - Findings**) How the denominator data is	None

Option	Description	Default
	grouped. For the available options, see Explore Data Source Options.	
Filters	(If **Type** is **Count**) Additional filters to use on the data source. For more information, see Filters. If **Data Type** is **Explore - Assets** or **Explore - Findings**, use the **Explore** query builder to define the filters. For more information, see Explore Data Source Options.	--
Numerator Filters	(If **Type** is **Ratio**) The filters to apply to the ratio numerator. For more information, see Filters. If **Data Type** is **Explore - Assets** or **Explore - Findings**, use the **Explore** query builder to define the filters. For more information, see Explore Data Source Options.	--
Denominator Filters	(If **Type** is **Ratio**) The filters to apply to the ratio denominator. For more information, see Filters. If **Data Type** is **Explore - Assets** or **Explore - Findings**, use the **Explore** query builder to define the filters. For more information, see Explore Data Source Options.	--
Rules		
Condition	Specifies the conditions for the matrix component. Use the drop-down menus to define the quantity and query value to use for the rule. Quantities: **Less than or equal to**, **Greater than or equal to**, **Exactly**, or **Not Equal to**.	--

Option	Description	Default
	Query values: **Events**, **Hosts**, **Vulnerabilities**, **Ports**, **Devices**, **Users**, **Alerts**, **Tickets**, **Assets**, or **Findings**. **Note:** The available query values depend on the **Data Type**. If **Data Type** is **Explore - Assets**, the only query value is **Assets**. If **Data Type** is **Explore - Findings**, the only query value is **Findings**. If **Group By** is **None** (the default), the cell counts assets or findings. If you select any other **Group By** option, the cell counts groups instead. For example, if you set **Group By** to **Operating System**, the cell counts the distinct operating systems that match the filters.	
Display	Specifies the appears of the matrix component when the rule **Condition** is met. • **Text** – Displays the **Query Value** or custom **User-Defined** text. • **Icon** – Displays the selected indicator icon. • (If **Type** is **Ratio**) **Indicator** – Displays a percentage.	Text
Text Color	(If **Display** is **Text**) The matrix component text color.	#1a1a40
Background	(If **Display** is **Text**) The matrix component background color.	#333333 or #ffffff

Line and Area Chart Component Options

Option	Description	Default
Data		
Date Type	The date type: • **Relative** – A date relative to the current time when the chart is loaded. • **Absolute** – An absolute time frame that is the same on each page visit.	Relative
Date Range	The date range for the line or area chart. If **Date Type** is **Relative**, select from the following options: • **Within *x* Minutes** – Display data within the last 15, 20, or 30 minutes. • **Within *x* Hours** – Display data within the last 1, 2, 4, 6, 12, 24, 48, or 72 hours. • **Within *x* Days** – Display data within the last 5, 7, 25, or 50 days. • **Within *x* Months** – Display data within the last 3 or 6 months. • **Within 1 Year** – Display data within the last year. If **Date Type** is **Absolute**, select a date and time for the beginning and end of the range.	Within 24 Hours
Series	Click to add a series to the line or area chart. For more information, see Line and Area Chart Series Options.	--

Line and Area Chart Series Options

Option	Description	Default

Name	The name of the series.	--
Data		
Data Type	The type of data: **Vulnerability** or **Explore - Findings**. **Explore - Assets** is not available for line and area chart series. For more information about Explore data sources, see Explore Data Source Options. **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
Source	(If **Data Type** is **Vulnerability**) Specifies the data source: **Cumulative** or **Mitigated**. **Explore - Findings** series always use cumulative data and do not have a **Source** option.	Cumulative
Query	(Not available if **Data Type** is **Explore - Findings**.) 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.	--
Group By	(If **Data Type** is **Explore - Findings**) How the data is grouped. **Severity** is the only option for line and area chart series.	Severity
Filters	Additional filters to use on the data source. For more information, see Filters. (If **Data Type** is **Explore - Findings**) Use the **Explore** query builder to define the filters that select the data to display. For	--

	more information, see Explore Data Source Options.	
Display		
Series Data	Data to display in the chart: **Total**, **Info**, **Low**, **Medium**, **High**, or **Critical**.	All

Configure a Simple Matrix Dashboard Component

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

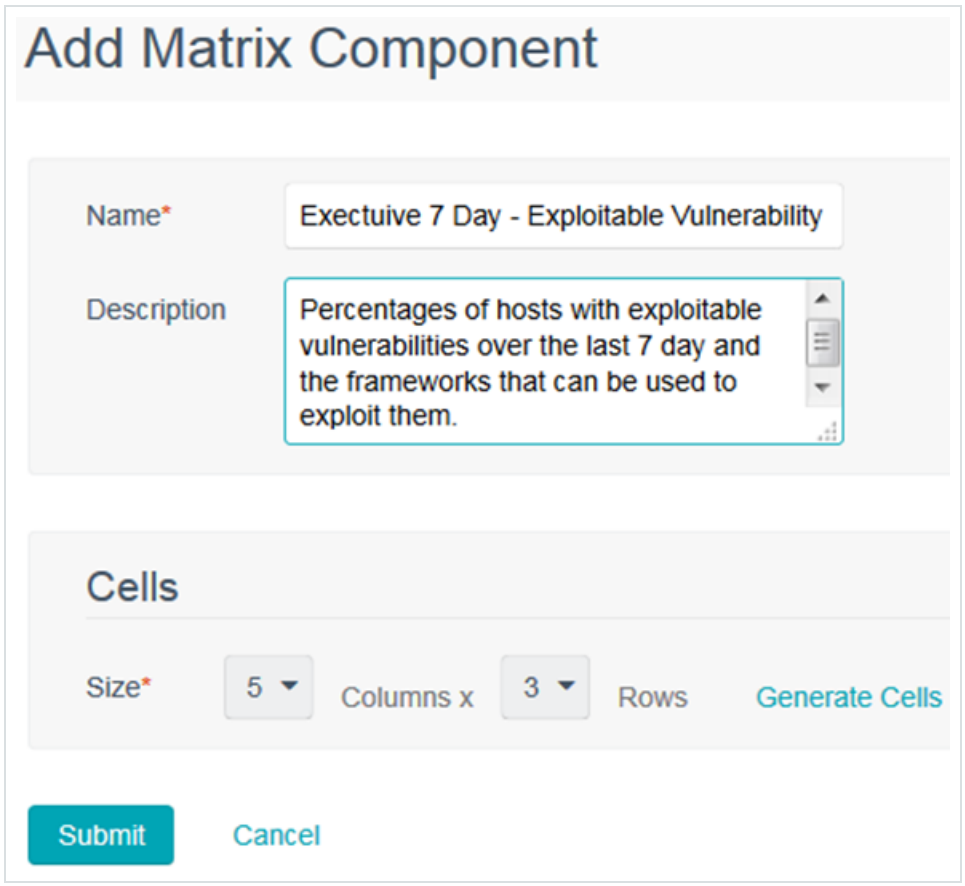
For more information, see Dashboards and Matrix Component Options.

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**.

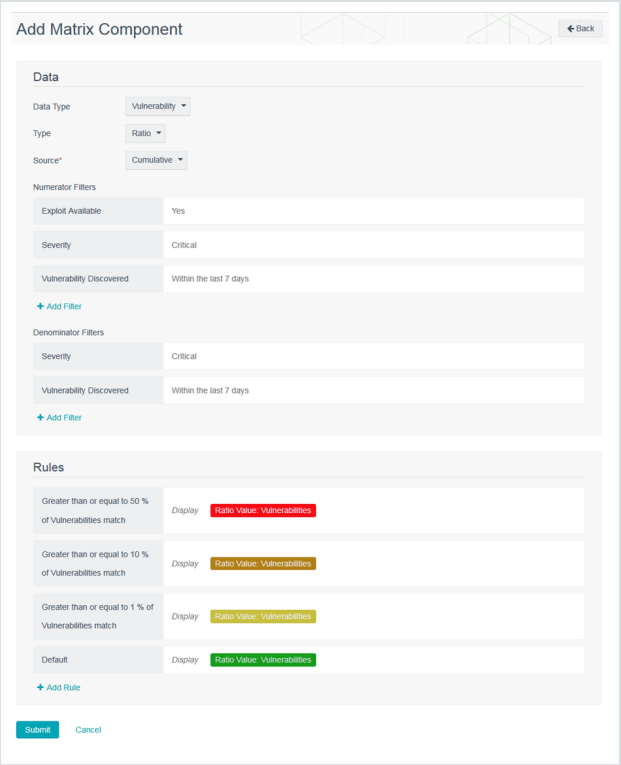
   The matrix editor appears, with the new header label displayed.



9. Repeat the header label steps for the other header cells.
10. Hover over the body cells and click the edit icon.

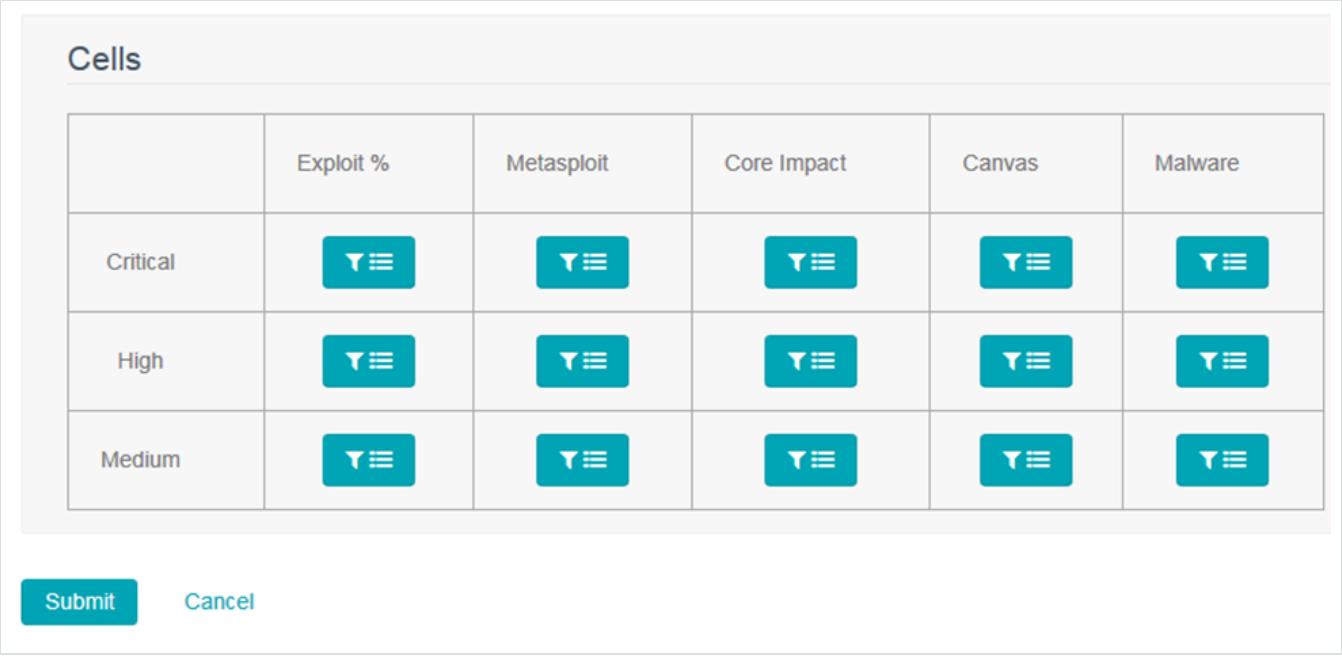
    The **Add Matrix Component** page appears.
11. Customize the matrix component options.

    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 discovered within the last 7 days. The Denominator filters are for vulnerabilities that have a Critical severity 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.

Explore

> **Note: Explore - Findings** is a preview feature. Some functionality may change before general availability.

The **Explore** section in Tenable Security Center Director is the central location for all your scan data. In **Explore**, you view and manage:

- *Assets*, resources of value on your network that require protection from threats, and
- *Findings*, single instances of vulnerabilities identified on those assets.

As Tenable sensors scan your environment or you import resources from other Tenable products, the system matches incoming data to existing resources or creates new resources. This data is presented on the **Assets** and **Findings** pages. There, using an intuitive query builder, you build lists of assets or findings to take action on. For example, you might export lists of assets to a file, or filter findings by repository and severity to focus on the highest-risk vulnerabilities in your environment.

You can also use asset and finding data from **Explore** in dashboard components. For more information, see Explore Data Source Options.

This guide explains how to use **Explore** and is arranged by the work you will do. Start with the following topics.

In This Topic	Learn How To...
Use the Assets Page	Perform common asset actions such as exporting lists, adding assets to scans, or viewing key details.
Use the Findings	View, filter, and export vulnerability findings across your repositories.

Page	
Asset Types	Understand asset types, including both licensed assets and assets which have not yet been scanned for vulnerabilities.
Asset Filters	Build lists of assets with filters ranging from when assets were first scanned to which operating system they run.
Findings Filters	Build lists of findings with filters including vulnerability severity and Common Platform Enumeration (CPE) ID.

Explore Assets

The **Explore-Assets** page in Tenable Security Center Director is the central location for all your scanned assets.

As Tenable Security Center Director scanners scan your environment or you import resources from other Tenable products, the system matches incoming data to existing resources or creates new resources. This data is presented on the **Explore-Assets** page. There, using an intuitive query builder, you build lists of assets to take action on. For example, you might export lists of assets to a file.

Assets are entities of value on your network that can be exploited. They include laptops, desktops, servers, routers, mobile phones, virtual machines, software containers, and cloud instances. Use the **Explore - Assets** page to view all the assets in your environment that Tenable Security Center Director has a record for. These are broken down into categories such as hosts, web applications, and network devices.

> **Note:** Tenable Security Center Director now processes **Explore** data requests in the background, allowing you to navigate to other screens while the results are generated and stored in a cache for up to 15 minutes.

The following topics explain how to view and export lists of assets, build custom queries with filters, and more.

Use the Explore - Assets Page

On the **Explore - Assets** page, you can view all the assets in your environment known to Tenable Security Center Director. These are broken down by asset type.

Note: Tenable Security Center Director ages out assets which have not been updated for more than 15 months.

Important: Due to differences in the asset source, asset counts within the **Tags** section may not match the asset counts within the Assets section of Tenable Security Center Director.

To view assets:

- In the left navigation, click **Explore** > **Assets**.

  The **Explore - Assets** page appears, showing licensed Host assets from the past 30 days.

On the **Explore - Assets** page, you can:

- View individual assets in a table with columns of information.
- At the top of the table, use the **Group By** drop-down to group the list of assets by **CVE**, **IAVM**, **Operating System**, **Asset Tag**, **Vulnerability Summary**, **ACR Severity**, **Microsoft ID**, **Network Summary**, or **System Type**.
- On the left, to refine the list of assets, choose an asset type.
- Click an individual asset to reveal a details pane.
- With the Query Builder, using asset filters, build custom queries.
- Select assets and add or remove labels.
- Export asset lists to CSV or JSON.
- Select an asset and view solutions for its vulnerabilities.
- In any asset row, click the drop-down **>** to reveal a list of related findings.
- In any asset row, use the menu ⋮ to access quick actions.

View Asset Details

On the **Explore - Assets** page, click an asset to open a pane of details. Then, click ⤢ to expand the pane.

The upper part of the **Asset Details** page contains the following information.

Attribute	Description
Name	The name of the asset; based on the presence of certain attributes in the following logical order: 1. Agent name 2. Local hostname 3. NetBIOS name 4. Fully Qualified Domain Name (FQDN) 5. IPv4 address 6. IPv6 address
Host ID	The unique identifier for the asset.
AES	(Requires Tenable Security Center+ license) The Tenable-defined Asset Exposure Score (AES) as an integer from 0 to 1000. For more information, see Asset Exposure Score in the *Tenable One Vulnerability Management User Guide*.
ACR	(Requires Tenable Security Center+ license) The Tenable-defined Asset Criticality Rating (ACR) as an integer from 1 to 10. For more information, see Asset Criticality Rating in the *Tenable One Vulnerability Management User Guide*.
Findings	The number of vulnerabilities identified on the asset.

The lower part of the **Asset Details** page is divided into sections. Not all information appears for all asset types.

Host Information

The **Host Information** section displays information about an asset, such as its operating system and the repository.

Attribute	Description
Name	The name of the asset based on the presence of certain attributes in the following logical order: • Agent name • Local hostname • NetBIOS name • Fully Qualified Domain Name (FQDN) • IPv4 address • IPv6 address
System Type	The device type, as reported by Plugin 54615.
Operating System	The operating system installed on the asset.
IP Addresses	The IPv4 or IPv6 address for the asset.
MAC Address	The MAC address for the asset.
Host ID	A UUID created for new assets during credentialed scans or agent scans. If an asset is found not to be unique, this UUID is not created and an existing one is reused.
Repository	The repository associated with the asset.

NetBIOS	The asset's unique NetBIOS ID.
DNS Name	The fully qualified domain name (FQDN) for the asset.
Key Drivers	Main drivers of the Asset Criticality Rating, as described in Tenable Lumin Metrics.
Compliance Data	Whether the scan that detected the vulnerability included compliance plugins.
Passive Data	Whether a passive scan detected the vulnerability.
CPE	A log of the Common Platform Enumeration (CPE) strings for the asset, identifying its software, hardware, or firmware using a standardized naming convention. This information is drawn from the National Vulnerability Database and Tenable's own plugins.

Scan Information

The **Scan Information** section displays information about the asset's scan history.

Attribute	Description
First Seen	The time and date when a scan first identified the asset.
Last Seen	The date and time of the scan that most recently identified the asset.
Source	The type of scanner that identified the asset.

Asset Types

The **Assets** page presents assets identified by scanners in Tenable Security Center Director or imported from other Tenable products.

Refine assets with filters in drop-downs > such as **By Source**. Or, use queries to apply additional filters. Choosing an asset type does not remove your current asset filters.

Asset Type	Description
By Source	**Assets broken down by the scanner that discovered or assessed the asset.**
Agent Scan	Assets discovered or assessed by Tenable Agents.
Nessus Scan	Assets discovered or assessed by Tenable Nessus.
NNM	Assets discovered or assessed by Tenable Network Monitor.
OT Scan	Assets discovered or assessed by Tenable One OT Exposure.
Web App Scan	Assets discovered or assessed by Tenable One Web App Scanning.
By Operating System	Assets broken down by operating system.
Windows	Assets running Microsoft Windows.
macOS	Assets running Apple MacOS.
Linux/Unix	Assets running Linux or Unix.
Other	Assets running another type of operating system.
By System Type	**Assets broken down by business and device function. Assets can only be in one system type.**
N/A	Assets without a type that the system cannot classify.
3D Printer	Devices that create three-dimensional objects from a digital file.
Access Control System	Assets that manage who has access to a resource, like a building

	or a network.
Access Point	Assets that provide a network connection point for other devices.
Accounting System	Assets that manage financial transactions and reports for an organization.
Actuator	Mechanical devices that use a power source to produce motion.
Analytics System	Assets that analyze data to provide insights and support decision-making.
Backplane Module	Circuit boards that provide a common bus for other modules to connect to.
Backup Agent	Software that facilitates data backups to a server.
Backup Server	Central servers that store and manage backed-up data.
Barcode Scanner	Assets that read and decode barcodes to retrieve information.
BMS Controller	Controllers for a Building Management System, managing building services like HVAC.
Camera	Assets that capture still images or video.
Computer Numerical Control (CNC)	Computer-automated manufacturing systems.
Consumer Storage	Storage devices for personal use, like external hard drives or USB drives.
Controller	Assets that control the behavior of other devices or systems.
Control Panel (CP)	Assets that provide an interface for a user to operate a system.

Converter	Assets that change one form of data into another.
CRM System	Assets that manage interactions with current and potential customers.
Database Server	Assets that store, retrieve, and manage databases.
Data Logger	Assets that record data over time or in relation to a specific location.
Directory Server	Assets that provide and manage information about network resources and users.
Distributed Control System (DCS)	Assets that control processes using distributed controllers.
Domain Controller	Servers that respond to security authentication requests within a computer domain.
DNS Server	Assets that translate human-readable domain names into IP addresses.
Drive	Assets that provide power and motion to a system.
Edge of Network	Assets at the periphery of a network, often processing data locally.
Embedded	Assets that are designed for a specific function within a larger mechanical or electronic system.
Embedded Print Server	Assets that are built into printers and enable network printing.
Engineering Station	Assets used to program, configure, and monitor industrial control systems.

Enterprise Storage	High-capacity, highly available storage systems for businesses.
ERP System	Assets that manage and integrate a company's business processes and data.
ERP System Client	User interfaces that connect to an ERP system.
Field Device	Devices, like sensors or actuators, that directly interact with a physical process.
File Server	Assets with centralized storage that provide access to files for multiple users over a network.
Firewall	Security systems that monitor and control incoming and outgoing network traffic.
Firewall VPN	Firewalls with integrated Virtual Private Network (VPN) functionality, securing and encrypting data communication.
Gaming Server	Servers designed for multiplayer video games, managing game state, and player connections.
Gateway	Network points that act as an entry and exit point for data.
General Purpose	Assets designed for a wide range of tasks rather than one specific function.
General Server	Servers that can host various applications and services without a specific role.
Helpdesk System	Software that manages support requests, tracking issues and their resolutions.
Historian	Centralized databases that collect and store time-stamped process data from industrial systems.

Hub	Networking devices that connect multiple devices, broadcasting data to all connected ports.
Human-Machine Interface (HMI)	User interfaces that connect an operator to a machine or system.
HVAC Module	Assets that control heating, ventilation, and air conditioning systems.
Hypervisor	Layers of software that create and run virtual machines.
Industrial Gateway	Assets designed for industrial environments to translate communication protocols between different networks.
Industrial Network Device	Network devices built to withstand harsh industrial conditions.
Industrial Printer	Robust printers designed for printing labels, barcodes, and other materials in industrial settings.
Industrial Router	Routers built to operate reliably in harsh industrial environments.
Industrial Sensor	Sensors designed for industrial use, measuring physical properties like temperature or pressure.
Industrial Switch	Network switches built to be reliable in industrial environments.
Input/Output (I/O)	Assets that communicate between a system and the outside world.
Intelligent Electronic Device (IED)	Microprocessor-based devices that control and monitor electrical equipment.
Internet of Things (IoT)	Assets that are part of a network of physical objects embedded with technology for communication.

Inverter	Devices that convert direct current (DC) to alternating current (AC).
IT Management System	Assets that help manage an organization's IT infrastructure and services.
KVM Switch	Hardware devices that allow users to control multiple computers from a single keyboard, video monitor, and mouse.
Lighting Control	Assets that manage and automate the operation of lights.
Load Balancer	Devices that distribute network traffic across multiple servers to ensure efficiency and reliability.
Mail Server	Servers that send, receive, and store emails.
Medical Device	Assets used for medical purposes, like diagnosis or therapy.
Misc	Miscellaneous or unclassified systems.
Mobile	Portable computing devices, like smartphones or tablets.
Multimedia Endpoint	Devices that capture or display multimedia content, such as a video conference camera or a digital sign.
Multimedia Stream Server	Servers that deliver video and audio content over a network in real time.
Multimedia Stream System	The complete infrastructure, including servers and endpoints, for streaming multimedia.
Network Access Control	Assets that restrict access to a network based on user or device identity.
Network Device	Assets that can connect to a computer network.

Network Router	Devices that forward data packets between computer networks.
Network Traffic Performance	Assets that measure and analyze data flow and efficiency on a network.
Network Switch	Assets that connect devices on a computer network, forwarding data to the intended destination.
OT Device	Assets used to monitor or control physical processes.
OT Server	Servers that host applications for operational technology, like SCADA or DCS.
OT Workstation	Workstations used by operators to manage and monitor industrial control systems.
Packet Shaper	Assets that control the flow of network traffic to prioritize certain data.
Panel	Control panels providing a user interface for operating a system.
Payment Card Industry (PCI)	Assets like card readers or terminals that protect sensitive cardholder data during a transaction.
Power Management	Assets that control and optimize a device's power usage.
Power Meter	Devices that measure electrical power consumption.
Power Supply	Components that supply electric power to an electrical load.
Private Branch eXchange (PBX)	Assets on private telephone networks used within a company.
Printer	Devices that produce hard copies of electronic documents.
Print Server	Servers that manage print jobs and connect network printers to

	client computers.
Programmable Logic Controller (PLC)	Assets used for automation of industrial processes.
Projector	Optical devices that project an image onto a surface.
Proxy Server	Intermediary servers that handle requests from clients seeking resources from other servers.
Optical Networking	Assets that use light to transmit data over fiber optic cables.
R&D Software	Software used for research and development activities, such as data analysis or simulation.
Radio	Assets that transmit or receive radio waves for communication.
Relay	Electrically operated switches that can control a circuit.
Remote Console Manager	Assets that allow remote access and control of a computer's console interface.
Remote I/O	Input/output systems located at a distance from the main controller.
Remote Terminal Unit (RTU)	Microprocessor-controlled devices that monitor and control field devices.
Repeater	Network devices that amplify and re-transmit a signal to extend its range.
Reverse Proxy Server	Servers that retrieve resources on behalf of a client from one or more servers.
Router	Assets that forward data packets between computer networks.

Robot	Programmable machines capable of carrying out complex actions automatically.
SCADA System	Assets used to monitor and control industrial processes in real time.
Security Appliance	Hardware devices designed for network security functions.
Security Gateway	Network devices that filter traffic to enforce security policies.
Serial Ethernet Bridge	Assets that convert serial data to Ethernet and vice versa.
Server	Assets that provide data and services to other computers.
Smart Hub	Central devices that connect and control smart home devices.
Smart Sensor	Sensors with integrated computing resources for data processing.
Smart TV	Televisions with integrated internet connections, providing access to streaming services.
Storage Device	Hardware devices used for storing digital data.
Supervisory Control and Data Acquisition (SCADA)	Supervisory Control and Data Acquisition (SCADA), a control system architecture.
Surveillance	Assets that monitor activities, such as cameras and recording equipment.
Switch	Assets that connect devices on a computer network, forwarding data to the intended destination.
Tablet	Portable computers with touchscreen interfaces, typically larger

	than a smartphone.
Telephony	Assets that transmit voice communications over a distance.
Teleconferencing	Assets that enable multiple people to communicate remotely via voice or video.
Tenable EM	Tenable Tenable Exposure Management, a platform that helps organizations gain visibility across the modern attack surface.
Tenable ICP	Tenable Industrial Control System Protection, a security solution for OT environments.
Tenable Sensor	Software or hardware components that collect security data for Tenable products.
Uninterruptible Power Supply (UPS)	Assets that provide emergency power to a load when the primary power source fails.
Universal Plug and Play (UPnP)	Assets that allow devices to discover and connect with each other automatically.
Unknown	Assets whose type cannot be identified.
Virtual Private Network (VPN)	Assets that facilitate a secure, encrypted connection over a public network.
Virtual Server	Software-based servers that operate as a separate server on a single physical machine.
Virtual Workstation	Software-based workstations that operate as a separate workstation on a single physical machine.
VoIP Device	Devices that use the internet for voice communication instead of a traditional telephone network.

Web Application Server	Servers that host web applications, processing requests and generating dynamic content.
Webcam	Video cameras that feed images to a computer or network in real time.
Web Server	Servers that store website files and deliver them to users via a web browser.
Wireless Access Point	Assets that allow wireless devices to connect to a wired network.
Wireless Access Point (WAP)	Assets that allow wireless devices to connect to a wired network.
Workstation	High-performance computers designed for technical or scientific applications.

Export Assets

You can export data to CSV format from the **Explore - Assets** page.

1. In the left navigation, click **Explore Assets**.

   The **Explore - Assets** page appears, showing licensed Host assets from the past 30 days.
2. Do one of the following:
   - To export a single asset:
     - Above the selected asset, the action bar appears. In the action bar, click [→ **Export**.
     - In the row for the asset that you want to export, click the ⋮ button.

       A menu appears.

       a. Click [→ **Export**.
   - Click on an asset to open that asset's Asset Details pane.

a. In the upper-right corner of the page, click the ⋮ button.

A menu appears.

b. Click [→ **Export**.

- To export multiple assets:

  a. In the asset list, select the checkbox next to each asset that you want to export.

  An action bar appears at the top of the list.

  b. In the action bar, click [→ **Export**.

The system processes the export and the file downloads to your computer. Processing may take several minutes.

Explore Assets Export Fields and Associated CSV Keys

On the **Export Assets** page you can export data from the **Explore - Assets** page in CSV format. When you export a CSV file, it will contain keys and their corresponding values. However, some of the keys used in the CSV may not clearly match the export fields selected for each Asset Type. The tables below provide a reference that maps the export fields to their corresponding CSV keys for each Asset Type.

Host Asset Export Mapping

The following table shows the mapping of each Host Audit Export Field to the associated key in the exported CSV file.

Host Asset Export Fields	Host Asset Export Keys
ACR	acr.score
ACR Calculated Score	acr.calculated_score
ACR Key Drivers	acr.drivers

Host Asset Export Fields	Host Asset Export Keys
AES	aes.score
AES Predicted	aes.is_predicted
Agent Name	agent_name
Asset ID	id
AWS Availability Zone	aws_availability_zone
AWS EC2 AMI ID	aws_ec2_instance_ami_id
AWS EC2 Instance ID	aws_ec2_instance_id
AWS EC2 Name	aws_ec2_name
AWS EC2 Product Code	aws_ec2_product_code
AWS Instance State	aws_ec2_instance_state_name
AWS Instance Type	aws_ec2_instance_type
AWS Owner ID	aws_owner_id
AWS Region	aws_region
AWS Security Group	aws_ec2_instance_group_names
AWS Subnet ID	aws_subnet_id
AWS VPC ID	aws_vpc_id
Azure Location	azure_location
Azure Resource Group	azure_resource_group

Host Asset Export Fields	Host Asset Export Keys
Azure Resource ID	azure_resource_id
Azure Resource Type	azure_type
Azure Subscription ID	azure_subscription_id
Azure VM ID	azure_vm_id
BIOS ID	bios_id
Provider	cloud.common.provider
Cloud Source	cloud_source
Created Date	created
Custom Attributes	custom_attributes
Disabled At	disabled_at
Discovery Information	discovery_information
DNS (FQDN)	display_fqdn
DNS List	fqdns
First Scan Time	first_scan_time
First Seen	first_observed
Google Cloud Instance ID	gcp_instance_id
Google Cloud Project ID	gcp_project_id
Google Cloud Zone	gcp_zone

Host Asset Export Fields	Host Asset Export Keys
Has Plugin Results	has_plugin_results
Has Agent	has_agent
Homepage Screenshot URL	homepage_screenshot_url
Host Name	host_name
Hosting Provider	hosting_provider
Installed Software	installed_software
IPv4 Address	ipv4_addresses
IPv6 Address	ipv6_addresses
Last Authenticated Scan	last_authenticated_scan_time
Last Licensed Scan	last_licensed_scan_time
Last Scan ID	last_scan_id
Last Scan Schedule ID	last_scan_schedule_id
Last Scan Target	last_scan_target
Last Scan Time	last_scan_time
Last Seen	last_observed
Licensed	is_licensed
MAC Address	display_mac_address
MAC Addresses	mac_addresses

Host Asset Export Fields	Host Asset Export Keys
Manufacturer TPM ID	tpm_id
Mitigations	mitigations
Name	name
NetBIOS Name	netbios_name
Network	network.id
Network Device Serial ID	network_device_serial_identifier
Observation Sources	observation_sources
Operating System	display_operating_system
Operating Systems	operating_systems
Ports	listening_ports
Protection Level	protection_level
Public	is_public
Region	cloud.runtime.region
Resource Category	cloud.common.resource_category
Resource Tags	cloud.common.resource_tags
Resource Type	cloud.common.resource_type
ServiceNow Sys ID	service_now_sys_id
Sources	sources

Host Asset Export Fields	Host Asset Export Keys
SSH Fingerprint	ssh_fingerprint
SSL/TLS	ssl_tls_enabled
System Type	system_type
Tags	tags
Tenable ID	tenable_id
Tenable Security Center Host ID	sc_host_uuid
Terminated At	terminated_at
Terminated By	terminated_by
Type	types
Updated Date	updated

Web Application Assets Export Mapping

The following table shows the mapping of each Web Application Finding Export Field to the associated key in the exported CSV file.

Web Application Asset Export Fields	Web Application Asset Export Keys
ACR	acr.score
ACR Calculated Score	acr.calculated_score
ACR Key Drivers	acr.drivers
AES	aes.score

Web Application Asset Export Fields	Web Application Asset Export Keys
AES Predicted	aes.is_predicted
Agent Name	agent_name
Asset ID	id
AWS Availability Zone	aws_availability_zone
AWS EC2 AMI ID	aws_ec2_instance_ami_id
AWS EC2 Instance ID	aws_ec2_instance_id
AWS EC2 Name	aws_ec2_name
AWS EC2 Product Code	aws_ec2_product_code
AWS Instance State	aws_ec2_instance_state_name
AWS Instance Type	aws_ec2_instance_type
AWS Owner ID	aws_owner_id
AWS Region	aws_region
AWS Security Group	aws_ec2_instance_group_names
AWS Subnet ID	aws_subnet_id
AWS VPC ID	aws_vpc_id
Azure Location	azure_location
Azure Resource Group	azure_resource_group
Azure Resource ID	azure_resource_id

Web Application Asset Export Fields	Web Application Asset Export Keys
Azure Resource Type	azure_type
Azure Subscription ID	azure_subscription_id
Azure VM ID	azure_vm_id
BIOS ID	bios_id
Provider	cloud.common.provider
Created Date	created
Custom Attributes	custom_attributes
Disabled At	disabled_at
Discovery Information	discovery_information
DNS (FQDN)	display_fqdn
DNS List	fqdns
First Scan Time	first_scan_time
First Seen	first_observed
Google Cloud Instance ID	gcp_instance_id
Google Cloud Project ID	gcp_project_id
Google Cloud Zone	gcp_zone
Has Agent	has_agent
Has Plugin Results	has_plugin_results

Web Application Asset Export Fields	Web Application Asset Export Keys
Homepage Screenshot URL	homepage_screenshot_url
Host Name	host_name
Hosting Provider	hosting_provider
Installed Software	installed_software
IPv4 Address	ipv4_addresses
IPv6 Address	ipv6_addresses
Last Authenticated Scan	last_authenticated_scan_time
Last Licensed Scan	last_licensed_scan_time
Last Scan ID	last_scan_id
Last Scan Schedule ID	last_scan_schedule_id
Last Scan Target	last_scan_target
Last Scan Time	last_scan_time
Last Seen	last_observed
Licensed	is_licensed
MAC Address	display_mac_address
MAC Addresses	mac_addresses
Manufacturer TPM ID	tpm_id
Mitigations	mitigations

Web Application Asset Export Fields	Web Application Asset Export Keys
Name	name
NetBIOS Name	netbios_name
Network	network.id
Network Device Serial ID	network_device_serial_identifier
Observation Sources	observation_sources
Operating System	display_operating_system
Operating Systems	operating_systems
Protection Level	protection_level
Public	is_public
Region	cloud.runtime.region
Resource Category	cloud.common.resource_category
Resource Tags	cloud.common.resource_tags
Resource Type	cloud.common.resource_type
ServiceNow Sys ID	service_now_sys_id
Sources	sources
SSH Fingerprint	ssh_fingerprint
SSL/TLS	ssl_tls_enabled
System Type	system_type

Web Application Asset Export Fields	Web Application Asset Export Keys
Tags	tags
Tenable ID	tenable_id
Tenable Security Center Host ID	sc_host_uuid
Terminated At	terminated_at
Terminated By	terminated_by
Type	types
Updated Date	updated

Asset Filters

On the **Assets** tab in **Explore** use the query builder to build custom queries that display the assets you need to see. You can use up to 35 filters in a custom query.

The following table defines the filters you can use. Not all filters are relevant for all asset types.

Filter	Description
ACR	(Requires Tenable Security Center+ license) Filters by the Tenable-defined Asset Criticality Rating (ACR) as an integer from 1 to 10. For more information, see Asset Criticality Rating in the *Tenable One Vulnerability Management User Guide*.
AES	(Requires Tenable Security Center+ license) Filters by the Tenable-defined Asset Exposure Score (AES) as an integer from 0 to 1000. For more information, see Asset Exposure Score in the *Tenable One Vulnerability Management User Guide*.

Filter	Description
AES Severity	(Requires Tenable Security Center+ license) Filters by the AES category of the AES calculated for the asset. For more information, see Asset Exposure Score in the *Tenable One Vulnerability Management User Guide*.
Application CPE	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 Tag	Filters by the tag assigned to the asset.
DNS Name	Filters by the fully-qualified domain name of the host that the vulnerability was detected on.
First Seen	Filters by the date and time when a scan first identified the asset.
Host ID	Filters by the UUID assigned to the asset by Tenable.
IAVM	Displays vulnerabilities based on one or more IVAM IDs. Type multiple IDs as a comma-separated list (e.g., *2011-A-0005,2011-A-0007,2012-A-0004*).
IP Addresses	Filters by the IPv4 address or IPv6 associated with the asset record.
Last Seen	Filters by the date and time at which the asset was last observed as part of a scan.
MAC Addresses	Filters by the MAC address associated with the asset record.
Name	Filters by the asset identifier, assigned based on the availability of the following attributes in order: Agent name, NetBIOS name, Local hostname, Fully Qualified Domain Name (FQDN), IPv4 address, and IPv6 address.

Filter	Description
NetBIOS	Filters by the NetBIOS name for the asset.
Operating System	Filters by the operating system(s) that a scan identified on the asset.
Plugin ID	Filters by the plugin ID or range based on a plugin ID. Available operators are equal to (=), not equal to (!=), greater than or equal (>=) and less than or equal to (<=).
Plugin Name	Using the **Contains** option, type all or a portion of the actual plugin name. For example, entering **MS08-067** in the plugin name filter displays vulnerabilities using the plugin named **MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)**. Similarly, entering the string **uncredentialed** displays a list of vulnerabilities with that string in the plugin name. Use the **Regex Match** option to filter plugin names based on Perl-compatible regular expressions (PCRE).
Port	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 than** or **less than** filters, only one port may be used. **Note:** All host-based vulnerability checks are reported with a port of 0 (zero).
Repository	Filters by assets associated with the chosen repository.
Severity	Displays vulnerabilities with the selected severity. For more information, see CVSS vs. VPR.

Filter	Description
Source	Filters by the type of scanner that identified the asset.
System Type	Filters by the system type.
Tenable ID	Filters by the UUID of the asset in Tenable Security Center Director.
Web App URL	**Required Additional License:** Tenable One Web App Scanning **Required Tenable Nessus Version:** 10.6.1 or later The URL for the discovered web application associated with the asset.

Asset Columns

On the **Assets** tab in **Explore**, you can view the assets in your environment. The **Assets** tab has the following columns, which you can show or hide by clicking **Columns** at the top of the table.

Column Field	Description
ACR	(Requires Tenable Security Center+ license) The Tenable-defined Asset Criticality Rating (ACR) as an integer from 1 to 10. For more information, see Asset Criticality Rating in the *Tenable One Vulnerability Management User Guide*.
AES	(Requires Tenable Security Center+ license) The Tenable-defined Asset Exposure Score (AES) as an integer from 0 to 1000. For more information, see Asset Exposure Score in the *Tenable One Vulnerability Management User Guide*.
DNS Name	The fully qualified domain name of the asset host. When processing fully qualified domain names (FQDNs) for host assets, Tenable Security Center

Column Field	Description
	Director normalizes all FQDNs to lowercase and then merges any duplicates.
MAC Address	A MAC address that a scan has associated with the asset record.
NetBIOS	The asset's NetBIOS name.
Host ID	The UUID assigned to the asset by Tenable.
Tenable ID	The UUID of the asset in Tenable Security Center Director.
Operating System	The operating system installed on the asset.
Repository	The repository associated with the asset.
System Type	The system type associated with the asset.
Last Seen	The date and time at which the asset was last observed as part of a scan.
Source	The type of scan that identified the asset.

Explore Findings

The **Explore - Findings** page is the central location for viewing vulnerability findings across your Tenable Security Center Director environment. Use the **Explore - Findings** page to search and filter your vulnerability data, identify security risks, and export findings for further analysis.

Findings are single instances of vulnerabilities on your assets, uniquely identified by plugin ID, port, and protocol. Every finding in Tenable Security Center Director belongs to a repository — the data store that holds the scan results for a given network segment or organizational unit.

Tenable Security Center Director automatically creates or updates findings when scans complete or you import scan results. Each finding is scoped to a repository. This means the **Explore - Findings**

page reflects the current state of your environment rather than the results of any individual scan. Retention is governed by your repository configuration.

The following topics explain how to view and export findings, filter results, work with finding details, and more.

Use the Findings Page

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

On the **Explore - Findings** page, you can view all cumulative vulnerability findings in your Tenable Security Center Director environment. Each finding is scoped to a repository.

To view your findings:

1. In the left navigation, click **Explore** > **Findings**.

   The **Findings** page appears.

On the **Findings** page, you can:

- View individual findings in a table with columns of information.
- Select an individual finding to reveal a details pane.
- In the Search bar, use findings filters to build custom queries.
- Build enhanced queries by using **Group By** options.
- Export findings to CSV.
- Share a filtered view by copying the page URL.
- Right-click any cell to use **Filter By** (apply that cell's value as a filter) or **Copy to Clipboard**.

The left navigation tree shows a fixed severity hierarchy. You cannot add or remove nodes.

- **Vulnerabilities**
  - By Severity
    - Critical
    - High
    - Medium
    - Low
    - Info

Three independent boolean attributes are available as filters: **Accept Risk**, **Recast Risk**, and **Mitigated**. The **Findings** page always shows cumulative findings – per-scan results are not surfaced here.

View Findings Details

> **Required User Role:** Read-Only, Basic User, Scan Operator, Standard User, Scan Manager, or Administrator

On the **Findings** page, click a finding to open a pane of details. The slideout URL follows the pattern /explore/findings/findingId/repositoryId/details.

The header of the details pane contains the following information.

Attribute	Description
Plugin Name	The name of the plugin that identified the vulnerability, for example Microsoft Netlogon Elevation of Privilege (Zerologon) (Remote).
Finding ID	The unique identifier (vulnUUID) for the finding.
Tenable Nessus Plugin ID	The numeric ID of the Tenable Nessus plugin. Links to the plugin page at tenable.com/plugins.

Severity	The vulnerability's CVSS-based severity (Critical, High, Medium, Low, Info).
Exploitability	Badges indicating exploitability characteristics, for example Remotely Exploitable, Locally Exploitable, Easy to Use, Functional, Proof of Concept, Exploited by Malware, Canvas, In the News.
VPR	The vulnerability's Vulnerability Priority Rating score.
CVSS v3	The CVSSv3 base score for the vulnerability.
ACR (Requires Tenable Security Center+)	The Asset Criticality Rating for the asset.

The lower part of the **Findings Details** page is divided into two tabs: **Details** and **Asset Summary**.

Details

The **Details** tab contains the following sections, in order.

Section	Description
Description	A description of the vulnerability. Includes a copy-to-clipboard control.
Plugin Output	Output from the plugin that identified the vulnerability.
Vulnerability Information	Important information about the vulnerability, including the following attributes: • **Severity** – The vulnerability's CVSS-based severity. • **Vulnerability Published** – The oldest date on which the vulnerability was either documented in an advisory or published in the National Vulnerability Database (NVD).

	• **Exploit Available** – Whether a known exploit exists. • **Patch Published** – The date a patch for the vulnerability was published. • **Exploitability Ease** – A description of how easy it is to exploit the vulnerability. • **Exploited With** – Exploit frameworks associated with the vulnerability. • **Port** – The port the scanner used to connect to the asset where the vulnerability was found. • **Protocol** – The protocol associated with the finding. • **CPE** – The Common Platform Enumeration identifier for the application.
Fixes	If available, details about fixes for the vulnerability, including: • **Solution** – A summary of how to officially remediate the vulnerability. • **See Also** – Links to websites with helpful information about the vulnerability.
Vulnerability Detection Timeline	Information about when the vulnerability was detected, including: • **First Seen** – The date when a scan first found the vulnerability on an asset. • **Last Seen** – The date when a scan last found the vulnerability on an asset. • **Last Fixed** – The date the finding was last marked as fixed. • **Vulnerability Age** – The age of a vulnerability based on its **State**. For *Active* vulnerabilities, based on the time elapsed between **First Seen** and today's date. For *Fixed* vulnerabilities, based on the time elapsed between **First Seen** and **Last Fixed** or the time elapsed between **Resurfaced** and **Last Fixed**. For *Resurfaced* vulnerabilities, based on

	the time elapsed between **Resurfaced** and and today's date.
VPR Key Drivers	Information about the key drivers Tenable uses to calculate a VPR for the vulnerability, including, but not limited to: • **CVE ID** – The CVE that is the primary contributor to the VPR score. • **VPR Severity** – The VPR severity categorization. • **VPR Percentile** – The score's percentile ranking relative to other vulnerabilities. • **Exploit Code Maturity** – Maturity of available exploit code. Options: **High**, **Functional**, **PoC**, **Unproven**. • **Exploit Probability** – Estimated probability of exploitation. • **Exploit Chain** – Whether the CVE is part of a known exploit chain. • **On CISA KEV** – Whether the CVE appears on the CISA Known Exploited Vulnerabilities catalog. • **In the News Intensity (Last 30)** – Volume of recent media coverage. • **In the News Recency** – Recency of media coverage. • **In the News Sources (Last 30)** – Categories of news sources referencing the CVE. • **Malware Observations Intensity (Last 30)** – Volume of malware observations. • **Malware Observations Recency** – Recency of malware observations. • **Targeted Industries** – Industries where attacks leveraging this CVE have been observed. • **Targeted Regions** – Geographic regions where attacks have been observed.
Plugin Details	Information about the plugin that detected the vulnerability, including: • **Plugin Family** – The family of the plugin that identified the

	vulnerability. • **Plugin Type** – The general type of plugin check (for example, `local` or `remote`). • **Plugin Publish Date** – The date on which the plugin that identified the vulnerability was published. • **Plugin Updated** – The date on which the plugin was last modified. • **Version** – The version of the plugin that identified the vulnerability.
CVEs	Per-CVE rows showing VPR, CVSS v2/v3/v4, EPSS, and EPSS percentile. Each row includes a link to the Tenable Security Center Director CVE search page for the CVE.
Risk Information	Information about the vulnerability's risk profile, including: • **CVSS v2 Severity (Risk Factor)** – The CVSS-based risk factor associated with the plugin. • **CVSSv2 Base Score** – The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments). • **CVSSv3 Base Score** – The CVSSv3 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments). • **CVSSv3 Vector** – A CVSSv3-based text string containing metric:value pairs to describe vulnerability characteristics, for example *AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H*. • **CVSSv4 Base Score** – The CVSSv4 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments). • **CVSSv4 Vector** – A CVSSv4-based text string containing metric:value pairs to describe vulnerability characteristics, for example

	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H. • **Plugin Publish Date** – The date the plugin was published. • **Version** – The plugin version.

Asset Summary

The **Asset Summary** tab contains details about the asset associated with the finding.

Section	Description
Asset Information	Information about the affected asset, including: • **Asset Name** – The name of the asset where a scan detected the vulnerability. This value is unique to Tenable One Vulnerability Management. • **IP Addresses** – The IPv4 address(es) for the affected asset. • **Asset ID** – The UUID of the asset where a scan detected the vulnerability. • **Operating System** – The operating system that the scan identified on the affected asset. • **DNS Name** – The fully qualified domain name of the asset host. • **MAC Addresses** – The MAC addresses for the affected asset. • **NetBIOS** – The NetBIOS name of the asset. • **Repository** – The repository that contains this finding. • **OS CPE** – The CPE identifier for the operating system. • **ACR** – The Asset Criticality Rating. Includes an **Edit** option if you have a Tenable Security Center+ license. • **ACR Source** – The source of the ACR value. • **Key Drivers** – The factors contributing to the ACR score.

	Includes an **Open in Assets** link that pivots to /explore/assets filtered by **Asset ID** and **Repository ID**.
Asset Tags	Asset Tags applied to the asset.
Last Seen	Information about when the affected asset was last identified on a scan, including: • **First Seen** – The date when a scan first found the vulnerability on an asset. • **Last Seen** – The date when a scan last found the vulnerability on an asset. • **Last Authenticated Scan** – The date and time of the last authenticated scan run against the asset. • **Last Unauthenticated Scan** – The date and time of the last unauthenticated scan run against the asset. • **Last Scan** – The date and time of the most recent scan of any type run against the asset. • **Scan Policy** – The scan policy used in the most recent scan. • **Source** – The source of the scan that detected the vulnerability on the affected asset, for example Tenable Nessus.

Using Group By Options on the Findings Page

The **Group By** feature in Tenable Security Center Director is a data organization tool used to consolidate the Findings table. Conceptually similar to a GROUP BY clause in a relational database query, this feature aggregates individual findings into logical categories, allowing you to pivot between different risk perspectives and streamline remediation workflows.

The **Group By** options appear above the findings table in **Explore > Findings**.

What is Group By?

The **Findings** table is a collection of finding instances. Every time a scanner identifies a security issue on an asset, it creates a unique, individual row in the table. While this provides total granularity, it can lead to a high volume of repetitive data when the same issue exists across many assets.

Group By allows you to consolidate these individual instances based on shared attributes. Instead of reviewing the same issue 100 times because it exists on 100 different computers, you can **Group By Plugin** to see it as a single line item with a count of affected assets. This transformation shifts your view from a list of detections to a list of actionable remediation tasks or prioritized assets.

Using Group By Options

1. On the **Findings** page, select a **Group By** option above the table.

   The table updates to show one row per grouped value, with a count of findings for each group.
2. Select the expand icon › on the left side of any row.

   A table appears that aggregates findings that a specific **Plugin ID** discovers across your entire environment into single rows. This shows the individual findings that make up that group, with granular details such as **IP Address**, **Port**, and **Repository**.

Group By Options

Tenable Security Center Director offers the following Group By options, all applying to vulnerability findings:

- **None** – The default view. Every finding is displayed as its own row, providing full granularity including port, protocol, IP address, and repository.
  - **Primary Use Case** – Technical verification, troubleshooting, or bulk export of all granular metadata across your entire finding set.
- **CVE** – Aggregates findings by CVE ID. Each row represents one CVE, with columns for Severity, VPR, EPSS, CVSS scores, and a total finding count.
  - **Primary Use Case** – Assess exposure to a specific CVE across all assets and repositories.

- **IAVM** – Aggregates findings by IAVM ID. Each row represents one IAVM advisory (DoD), with CVSS and VPR scores and a total count.
    - **Primary Use Case** – Track compliance against DoD IAVM requirements.
- **Vulnerability** – Groups all instances of a specific plugin (Plugin ID + Plugin Name) across your environment into a single row. This is a root cause view.
    - **Primary Use Case** – Determine the blast radius of a specific vulnerability and identify the most impactful remediation action, such as a specific patch.
- **Severity** – Groups findings by severity bucket (Critical, High, Medium, Low, Info). Each row shows the count of findings at that level.
    - **Primary Use Case** – Get a high-level overview of risk distribution across your environment.
- **Operating System** – Groups findings by the operating system detected on affected assets. Includes a Detection Method column.
    - **Primary Use Case** – Identify which OS platforms carry the most risk and prioritize OS-level patching or hardening.
- **Asset** – Aggregates all findings onto the specific asset where they were discovered. Each row represents a unique asset with severity counts.
    - **Primary Use Case** – Assess the total risk profile of individual devices and prioritize asset-level remediation.
- **Asset Tag** – Groups findings by asset tag, with severity counts per tag. Each row represents a tag applied to one or more assets.
    - **Primary Use Case** – Assess risk by logical grouping (for example, by business unit, location, or environment) using tags assigned to assets.

Group By to Promote Ease of Use

Here are examples of how **Group By** can improve your daily workflow.

- **Reduced Noise** – Clears potential clutter of seeing repetitive findings, allowing you to see the true scope of your exposure.

- **Faster Prioritization** – You can immediately see which specific vulnerability (Vulnerability), CVE (CVE), or server (Asset) represents the highest concentrated risk.
- **Role-Based Views**
    - Remediation teams can **Group by Vulnerability** to see what plugins need to be addressed and how many assets are affected.
    - System owners can **Group By Asset** to see the total risk profile of the specific machines they manage.
    - Security managers can **Group By Asset Tag** to assess risk across logical groups such as business units or environments.
    - DoD teams can **Group By IAVM** to track findings against specific IAVM advisories.

Export Findings

You can export findings data to CSV from the **Findings** page. Exports are scoped to the current filter state and Group By selection.

There are two export variants:

- **Export all** – exports all findings matching the current filters. If the result set exceeds the export size limit, an **Export Limit** box appears.
- **Export selected** – exports only the rows you have selected in the grid.

The exported filename follows the pattern: `explore-findings-groupBy[-selected]-ISO timestamp.csv`

To export findings from the **Findings** page:

1. In the left navigation, click **Explore** > **Findings**.
2. Select one or more findings to export by doing one of the following:
    - To export all findings matching your current filters, click **Export** in the toolbar without selecting any rows.

- To export selected rows, select the checkbox for each row you want to export, then click **Export** in the toolbar.

An **Export Started** notification appears immediately. When the file is ready, an **Export Complete** notification appears and the CSV file downloads to your computer.

Findings Filters

On the **Findings** page in **Explore**, use the Search bar to build filter queries that return the findings you need to see. For enhanced filtering, combine filters with Using Group By Options on the Findings Page.

> **Note:** The **Findings** page always displays cumulative findings.

The following table lists the filters available on the Findings page. All filters apply to vulnerability findings.

Filter	Description
Accept Risk	Whether the finding has an active accept-risk acknowledgement. Options: **Yes**, **No**.
ACR Score	(Requires Tenable Security Center+ license) Filters by the Tenable-defined Asset Criticality Rating (ACR) as an integer from 1 to 10. For more information, see Asset Criticality Rating in the *Tenable One Vulnerability Management User Guide*.
AES Severity	(Requires Tenable Security Center+ license) Filters by the AES category of the AES calculated for the asset. For more information, see Asset Exposure Score in the *Tenable One Vulnerability Management User Guide*.
Application CPE	Allows a text string search to match against available CPEs. The filter may

Filter	Description
	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 ID	The unique identifier (UUID) of the asset where the finding was detected.
Asset Tag	Filters by the tag assigned to the asset.
CVE Category	(Requires Vulnerability Intelligence license) Options: **in_the_news**, **ransomware**, **emerging_threats**, **persistently_exploited**, **cisa_known_exploitable**, **recent_active_exploitation**, **top_50_vpr**.
CVE ID	The CVE identifier associated with the vulnerability.
CVSSv2 Base Score	The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).
CVSSv2 Vector	A CVSSv2-based text string containing metric:value pairs to describe vulnerability characteristics, for example *AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H*.
CVSSv3 Base Score	The CVSSv3 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).
CVSSv3 Vector	A CVSSv3-based text string containing metric:value pairs to describe vulnerability characteristics, for example *AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H*.
CVSSv4 Base Score	The CVSSv4 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).
CVSSv4	The CVSS v4 supplemental vector string.

Filter	Description
Supplemental	
CVSSv4 Threat Score	Numeric CVSS v4 threat score. Supports the `between` operator.
CVSSv4 Threat Vector	The CVSS v4 threat vector string.
CVSSv4 Vector	The CVSS v4 base vector string.
DNS Name	The fully qualified domain name of the asset host.
EPSS Score	The Exploit Prediction Scoring System (EPSS) probability score. Supports the `between` operator.
Exploit Available	Whether a known exploit exists for the vulnerability. Options: **Yes**, **No**.
Exploit Code Maturity	Maturity of available exploit code (VPR key driver). Options: **Functional**, **High**, **POC**, **Unproven**.
Exploit Frameworks	The exploit framework(s) associated with the vulnerability.
Finding ID	The unique identifier (vulnUUID) for the finding.
First Seen	The date the finding was first detected. Supports date range operators.
IAVM ID	The Information Assurance Vulnerability Management (IAVM) identifier for the vulnerability.
IP Addresses	The IPv4 address of the asset where the finding was detected. Supports CIDR notation.
Last Seen	The date the finding was most recently detected. Supports date range

Filter	Description
	operators.
MAC Addresses	The MAC address of the asset where the finding was detected.
Microsoft ID	The Microsoft security bulletin or advisory ID associated with the vulnerability.
Mitigated	Whether the finding has been remediated or patched. Options: **Yes**, **No**.
NetBIOS Name	The NetBIOS name of the asset where the finding was detected.
On CISA KEV	Whether the vulnerability appears on the CISA Known Exploited Vulnerabilities catalog (VPR key driver). Options: **Yes**, **No**.
Operating System	The operating system detected on the asset where the finding was identified.
Patch Published	The date a patch was published for the vulnerability. Supports date range operators.
Plugin Family	The plugin family that contains the plugin which identified the vulnerability. Active, passive, and Tenable One Web App Scanning families are distinguished by family ID range; passive families include a (Passive) suffix and Tenable One Web App Scanning families include a (WAS) suffix.
Plugin ID	The numeric ID of the Tenable Nessus plugin that identified the vulnerability.
Plugin Modified	The date the plugin was last updated. Supports date range operators.
Plugin Name	The name of the plugin that identified the vulnerability.
Plugin Output	The text output produced by the plugin when it detected the vulnerability.

Filter	Description
(Plugin Text)	
Plugin Published	The date the plugin was originally published. Supports date range operators.
Plugin Type	The general type of plugin check. Options: **active**, **passive**, **WAS**.
Port	The port on the asset where the finding was detected.
Protocol	The network protocol associated with the finding. Options: **Unknown**, **ICMP**, **TCP**, **UDP**.
Recast Risk	Whether the finding has an active recast-risk override. Options: **Yes**, **No**.
Repository ID	The repository that contains the finding.
Risk Factor	The CVSS v2 severity bucket. Options: **Critical**, **High**, **Medium**, **Low**, **Info**, **None**.
Severity	The vulnerability severity level. Multi-select. Options: **Critical**, **High**, **Medium**, **Low**, **Info**.
Targeted Industries	Industries where threat actors have observed attacks leveraging the CVE (VPR key driver).
Targeted Regions	Geographic regions where threat actors have observed attacks leveraging the CVE (VPR key driver).
VPR Score	The Vulnerability Priority Rating (VPR) score. Supports the `between` operator.
VPR Severity	The VPR severity category (VPR key driver). Options: **Critical**, **High**, **Medium**, **Low**, **Info**.

Filter	Description
Vuln UUID (Finding ID)	The vulnUUID unique identifier for the finding.
Vulnerability Published	The date the vulnerability was publicly disclosed. Supports date range operators.

Findings Columns

On the **Findings** page in **Explore**, the available columns depend on the active Group By selection. You can show or hide columns using the column chooser. Column visibility and order do not persist across page reloads.

None

Column	Description
ACR	(Requires Tenable Security Center+ license) The Tenable-defined Asset Criticality Rating (ACR) as an integer from 1 to 10. For more information, see Asset Criticality Rating in the *Tenable One Vulnerability Management User Guide*.
AES	(Requires Tenable Security Center+ license) The AES category of the AES calculated for the asset. For more information, see Asset Exposure Score in the *Tenable One Vulnerability Management User Guide*.
Asset Name	The name of the asset where the finding was detected.
CGI Scan Enabled	Whether the scan policy had CGI scanning enabled.

Column	Description
DNS Name	The DNS hostname of the asset.
EPSS	The Exploit Prediction Scoring System probability score for the vulnerability.
Finding ID	The unique identifier (vulnUUID) for the finding.
Host ID	The asset UUID (host UUID).
IP Addresses	The IPv4 address(es) of the asset.
MAC Addresses	The MAC address of the asset.
NetBIOS Name	The NetBIOS name of the asset.
Paranoid Scan Enabled	Whether the scan policy had paranoid scanning enabled.
Plugin Family	The plugin family that contains the plugin which identified the vulnerability.
Plugin ID	The numeric ID of the Tenable Nessus plugin that identified the vulnerability.
Plugin Name	The name of the plugin that identified the vulnerability.
Port	The port on the asset where the finding was detected.
Protocol	The network protocol associated with the finding.
Repository	The repository that contains the finding.
Severity	The vulnerability severity level (Critical, High, Medium, Low, Info).
Tenable ID	The Tenable UUID for the finding.

Column	Description
Thorough Scan Enabled	Whether the scan policy had thorough scanning enabled.
VPR	The Vulnerability Priority Rating (VPR) score for the vulnerability.

Asset

Column	Description
ACR	(Requires Tenable Security Center+ license) The Tenable-defined Asset Criticality Rating (ACR) as an integer from 1 to 10. For more information, see Asset Criticality Rating in the *Tenable One Vulnerability Management User Guide*.
AES	(Requires Tenable Security Center+ license) The AES category of the AES calculated for the asset. For more information, see Asset Exposure Score in the *Tenable One Vulnerability Management User Guide*.
Asset ID	The unique identifier (UUID) of the asset.
Asset Name	The name of the asset where the finding was detected.
Critical	The count of Critical severity findings on the asset.
DNS	The DNS hostname of the asset.
First Seen	The date the asset was first seen.
High	The count of High severity findings on the asset.
Info	The count of Info severity findings on the asset.

Column	Description
IP Addresses	The IPv4 address(es) of the asset.
Last Seen	The date the asset was most recently seen.
Low	The count of Low severity findings on the asset.
MAC	The MAC address of the asset.
Medium	The count of Low severity findings on the asset.
NetBIOS	The NetBIOS name of the asset.
Operating System	The operating system detected on the asset.
Repository	The repository that contains the asset's findings.
Score	The aggregate risk score for the asset.
Total	Aggregate risk score for the asset.
UUID	The asset UUID.

Asset Tag

Column	Description
Asset Tag	The name of the asset tag.
Critical	The count of Critical severity findings on the asset.
High	The count of High severity findings on the asset.
Info	The count of Info severity findings on the asset.

Column	Description
Low	The count of Low severity findings on the asset.
Medium	The count of Low severity findings on the asset.
Score	The aggregate risk score for the asset.
Total	Aggregate risk score for the asset.

CVE

Column	Description
CVE ID	The CVE identifier.
CVSS v2	The CVSS v2 base score for the CVE.
CVSS v3	The CVSS v3 base score for the CVE.
CVSS v4	The CVSS v4 base score for the CVE.
EPSS	The EPSS probability score for the CVE.
Severity	The severity level of the CVE.
Total	Total count of findings associated with the CVE.
VPR	The Vulnerability Priority Rating (VPR) score for the CVE.

IAVM

Column	Description
CVSS v2	The CVSS v2 base score for the IAVM.

Column	Description
CVSS v3	The CVSS v3 base score for the IAVM.
CVSS v4	The CVSS v4 base score for the IAVM.
EPSS	The EPSS probability score for the IAVM.
IAVM	The IAVM identifier.
Severity	The severity level of the IAVM.
Total	Total count of findings associated with the IAVM.
VPR	The Vulnerability Priority Rating (VPR) score for the IAVM.

Operating System

Column	Description
Critical	The count of Critical severity findings on the operating system.
Detection Method	How the operating system was detected.
High	The count of High severity findings on the operating system.
Info	The count of Info severity findings on the operating system.
Low	The count of Low severity findings on the operating system.
Medium	The count of Low severity findings on the operating system.
Operating System	The name of the operating system.
Score	The aggregate risk score for the operating system.
Total	Total count of findings across all severities for this operating system.

Severity

Column	Description
Count	The number of findings at this severity level.
Severity	The severity level (Critical, High, Medium, Low, Info).

Vulnerability (Plugin)

Column	Description
EPSS	The EPSS probability score for the plugin.
Last Modified	The date the plugin was last modified.
Patch Date	The date a patch was published for the vulnerability.
Plugin Family	The plugin family.
Plugin ID	The numeric ID of the plugin.
Plugin Name	The name of the plugin.
Plugin Publish Date	The date the plugin was originally published.
Severity	The vulnerability severity level (Critical, High, Medium, Low, Info).
Total	Total count of findings for this plugin across all assets.
VPR	The Vulnerability Priority Rating (VPR) score for the vulnerability.
Vulnerability Publish Date	The date the vulnerability was publicly disclosed.

Scan Results

The **Scan Results** page displays scan results and statuses from scans running on your managed Tenable Security Center instances.

Note: When you upgrade to Tenable Security Center Director 6.7.x, you must sync existing remote repositories before you browse vulnerability data from newly synced scan results.

Note: For each agent synchronization job result for a child node, Tenable Security Center imports a metadata record containing no vulnerability data. This metadata record appears as a second result on the **Scan Results** page. To prevent Tenable Security Center from importing the metadata file, configure and launch agent scans from Tenable Security Center, as described in Agent Scans.

For more information, see Manage Scan Results.

Scan Result Statuses

You can view the scan status and the import status for scans running on your managed Tenable Security Center instances, as described in View Scan Result Details.

Scan Status

The scan status specifies the status of the scan.

Status	Description
Active Scans	
Queued	The scan is queued.
Preparing	Tenable Security Center is preparing to run the scan.
Resolving Hostnames	Tenable Security Center is resolving hostnames before running the scan.
Verifying Targets	Tenable Security Center is verifying targets before running the scan.

Status	Description
Initializing Scanners	Tenable Security Center is initializing scanners before running the scan.
Running	The scan is running.
Pausing	You paused the scan and Tenable Security Center is pausing the scan.
Paused	The scan is paused.
Resuming	You resumed the scan and Tenable Security Center is resuming the scan.
Stopping	Tenable Security Center is stopping the scan.
Completed	The scan finished successfully.
Partial	The scan finished and some results are available.
Error	The scan did not finish. Common causes include: • The Nessus scanner is unreachable or disconnected. • The scanner ran out of disk space or memory during the scan. • A network timeout or connectivity issue occurred during the scan. • The scan was stopped by the system due to a resource constraint. Do any of the following: • Check the scan result for an error code and recommended action. For more information, see Error Messages. • Verify that the Nessus scanner is connected and has sufficient disk space and memory. • Review the Tenable Security Center logs for details. For more information, see System Logs. • Retry the scan. If the error persists, contact Tenable Support.

Status	Description
Agent Scans	
Queued	The scan is queued.
Running	The scan is running.
Completed	The scan finished successfully.
Error	The scan did not finish. Common causes include: • The Nessus scanner is unreachable or disconnected. • The scanner ran out of disk space or memory during the scan. • A network timeout or connectivity issue occurred during the scan. • The scan was stopped by the system due to a resource constraint. Do any of the following: • Check the scan result for an error code and recommended action. For more information, see Error Messages. • Verify that the Nessus scanner is connected and has sufficient disk space and memory. • Review the Tenable Security Center logs for details. For more information, see System Logs. • Retry the scan. If the error persists, contact Tenable Support.

Import Status

The scan status specifies the status of the scan result import to Tenable Security Center.

Status	Description
Active and Agent Scans	
No Results	The scan finished successfully but yielded no results.
Import Pending	Tenable Security Center is preparing to start the import.
Importing	Tenable Security Center is importing the scan result data.
Finished	The import finished successfully.
Blocked	Tenable Security Center did not import the scan result for one of the following reasons: • You have exceeded your license limit. • The scan result import would cause you to exceed your license. For more information about license limits, see License Requirements. **Note:** After you update your license, you may need to run or import blocked scans again.
Error	The import did not finish. Common causes include: • Insufficient disk space on the Tenable Security Center server or in the target repository. • The scan result file is corrupted or in an unsupported format. • A database error occurred during import. • The target repository is unavailable or has been deleted. Do any of the following: • Verify that the Tenable Security Center server has sufficient disk space.

Status	Description
	• Try importing the scan result again. For more information, see Manage Scan Results. • Review the Tenable Security Center logs for details. For more information, see System Logs. • If the error persists, contact Tenable Support.

Availability

The scan result availability specifies whether the scan result can be viewed in Tenable Security Center Director.

Status	Description
Available	Tenable Security Center Director successfully imported the scan result data. **Note:** By default, Tenable Security Center Director retains scan results from managed Tenable Security Center instances for 30 days. For more information, see Data Expiration Settings.
Syncing	Tenable Security Center Director is importing the scan result data from a managed Tenable Security Center instance.
Not Synced	The scan result is not imported to Tenable Security Center Director. If the scan status is **Partial** or **Completed**, you can manually retrieve the scan result. For more information, see Retrieve a Scan Result From Managed Tenable Security Center.

Manage Scan Results

Required Tenable Security Center 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 (for example, you cannot download results for a scan with errors).

For more information, see Scan Results.

View Scan Results

Note: For each agent synchronization job result for a child node, Tenable Security Center imports a metadata record containing no vulnerability data. This metadata record appears as a second result on the **Scan Results** page. To prevent Tenable Security Center from importing the metadata file, configure and launch agent scans from Tenable Security Center, as described in Agent Scans.

To view a list of scan results:

1. Log in to Tenable Security Center 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.
   - **Availability** – The status of the scan result. For more information, see Scan Result Statuses.
   - **Tenable.sc Instance** – The name of the Tenable Security Center instance where the scan was run.
   - **Type** – The type of scan that generated the scan result.
   - **Scan Policy** – The name of the scan policy that generated the scan result.
   - **Scanned IPs** – The number of IP addresses scanned.
   - **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 Security Center 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 Security Center instance, see Retrieve Scan Results.
5. To view a set of scan results:
   a. Right-click the row for the scan.

      The actions menu appears.

      -or-

      Select the check box for the scan.

      The available actions appear at the top of the table.

   b. Select **Browse**.

      The Vulnerability Summary analysis tool appears, populated with data from the scan.
6. To view additional details for a scan result, see View Scan Result Details.

View Scan Result Details

You can view details for any scan result. For more information, see Scan Results.

To view scan result details:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Scan Results** (administrator users) or **Scans** > **Scan Results** (organizational users).

   The **Scan Results** page appears.
3. Right-click the row for the scan result.

   The actions menu appears.

   -or-

   Select the check box for the scan result.

The available actions appear at the top of the table.

4. Click **View**.

   The **View Scan Result** page appears.

Section	Action
General	View general information for the scan result. • **Name** – The scan result name. • **Type** – The type of scan that generated the scan result. • **Tenable Security Center Instance** – The name of the Tenable Security Center instance where the scan was run. • **Scan Policy** – The name of the scan policy that generated the scan result. • **Repository** – The name of the repository associated with the scan policy that generated the scan result. • **Scanned IPs / Total IPs** – The number of IP addresses scanned compared to the total number of IP addresses targeted in the scan. • **Status** – The scan status. For more information, see Scan Status. • **Scanner Summary** – The name of the scan and how many IPs were scanned. • **Start Time** – The date and time Tenable Security Center started the scan. • **Finish Time** – The date and time Tenable Security Center completed the scan. • **Status** – The scan status. For more information, see Scan Status. • **Duration** – The total time elapsed while running the scan. • **Import Start** – The date and time Tenable Security Center started the

Section	Action
	scan result import. • **Import Finish** – The date and time Tenable Security Center completed the scan result import. • **Import Status** – The scan result import status. For more information, see Import Status. • **Import Duration** – The total time elapsed during scan result import. • **Owner** – The username for the user who added the scan. • **Group** – The group associated with the scan. • **ID** – The scan result ID.

Filter Scan Results

To filter scan results:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Scan Results** (administrator users) or **Scans** > **Scan Results** (organizational users).

   The **Scan Results** page appears.
3. To filter the scan results:

   Click the filter icon. Filters allow you to view only desired scan results. Filter parameters include:

   - **Access** - filters by whether the scan is manageable or usable.
   - **Group** - filters by the groups that can access the scans.
   - **Name** - filters by the scan name.
   - **Owner** - filters by the scan owner.
   - **Scan Policy** - filters by the scan policy.
   - **Status** - filters by the scan status.

- **Time (Created)** - filters by when the scan result was created.
- **Time (Finished)** - filters by when the scan finished running.
- **Type** - filters by the type of scan.

4. 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 gray next to the filter displays how many filters are currently in use.

Retrieve a Scan Result From Managed Tenable Security Center

To retrieve a scan result from a managed Tenable Security Center instance:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Scan Results** (administrator users) or **Scans** > **Scan Results** (organizational users).

   The **Scan Results** page appears.
3. Right-click the row for a **Partial** or **Completed** scan that is **Not Synced**.

   The actions menu appears.

   -or-

   Select the check box for a **Partial** or **Completed** scan that is **Not Synced**.

   The available actions appear at the top of the table.
4. Click **Retrieve**.

   Tenable Security Center Director imports the scan result.

   Note: By default, Tenable Security Center Director retains scan results from managed Tenable Security Center instances for 30 days. For more information, see Data Expiration Settings.

Download Scan Results

To download scan results:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Scan Results** (administrator users) or **Scans** > **Scan Results** (organizational users).

   The **Scan Results** page appears.
3. Right-click the row for the scan.

   The actions menu appears.

   -or-

   Select the check box for the scan.

   The available actions appear at the top of the table.
4. Select **Download**.

   Tip: On a standard scan, you can download a Tenable Nessus results file. If the scan contains SCAP results, you can use an additional option to download the SCAP results.

Send a Copy of Scan Results

To send a copy of the scan results to users without access to Tenable Security Center Director:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Scan Results** (administrator users) or **Scans** > **Scan Results** (organizational users).

   The **Scan Results** page appears.
3. Right-click the row for the scan.

   The actions menu appears.

   -or-

   Select the check box for the scan.

   The available actions appear at the top of the table.
4. Select **Email**.

Generate a Report for Scan Results

To generate a report for the scan results based on a preconfigured report:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Scan Results** (administrator users) or **Scans** > **Scan Results** (organizational users).

   The **Scan Results** page appears.
3. Right-click the row for the scan.

   The actions menu appears.

   -or-

   Select the check box for the scan.

   The available actions appear at the top of the table.
4. Select **Send to Report**.

   Tenable Security Center Director sends the scan results to a report.

Pause or Resume a Scan

To pause or resume a running scan:

1. Log in to Tenable Security Center 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, click the pause or play button, as described in Start or Pause a Scan.

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 Tenable Security Center 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 Security Center 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 Asset Tags.
4. To customize the table, see Interact with a Customizable Table.
5. 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 Security Center 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.
   - **EPSS** – The EPSS score for the vulnerability.

- **CVSSv3 Base Score** – The highest CVSSv3 or CVSS 4 score for a vulnerability included in the solution. If only CVSSv2 or CVSS v4 is available, the column is blank.
- **CVSSv4 Base Score** – The CVSSv4 score for the vulnerability included in the solution. If only CVSSv2 or CVSSv3 is available, the column is blank.

6. To view details for a solution, click a row.

   The **Solution Details** page appears. For more information, see Solution Details.

View Solution Details

> **Required Tenable Security Center 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 export the details for a solution, see Export Hosts Affected by a Solution.

To view details for a specific solution:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Solutions**.

   The **Solutions** page appears.
3. Click a solution row.

   The **Solution Details** page appears.

Section	Action
Metrics summary	View summary statistics for the recommended solution. • **Hosts Affected** – The number of devices affected by the solution. • **Vulnerabilities** – The total number of vulnerability instances included in the solution.

Section	Action
	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.
Vulnerabilities Included table	View all vulnerabilities related to the recommended solution, sorted by decreasing VPR. • **Plugin** – The plugin ID. • **Hosts Affected** – The number of devices affected by the solution. • **VPR** – The VPR for the vulnerability. • **EPSS** – The EPSS score for the vulnerability. • **CVSSv3 Base Score** – The CVSSv3 score for the vulnerability included in the solution. If only CVSSv2 or CVSS v4 is available, the column is blank. • **CVSSv4 Base Score** – The CVSSv4 score for the vulnerability included in the solution. If only CVSSv2 or CVSSv3 is available, the column is blank.
Hosts Affected table	View device information. • **IP Address** – The IP address for the device. • **NetBIOS** – The NetBIOS name, if known.

Section	Action
	• **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.

What to do next:

- (Optional) Export the hosts affected by the solution to share with others in your organization, as described in Export Hosts Affected by a Solution.

Export Hosts Affected by a Solution

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

You can export a list of hosts affected by a solution as a `.csv` file to share the data with others in your organization. For more information, see Solutions Analysis.

To export hosts affected by a solution:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Solutions**.

   The **Solutions** page appears.
3. Click the row for the solution for which you want to export a list of affected hosts.

   The **Solution Details** page appears.
4. In the upper-right corner, click **Export as CSV**.

   A confirmation window appears.

Note: If the number of affected hosts is greater than 1,000, Tenable Security Center Director prompts you to type a name for the CSV report result you want to generate. After generation, you can download the report result, as described in Download a Report Result.

5. Select or clear the check boxes to indicate which columns you want to appear in the exported file.

Column Name	Description
Solution ID	The plugin ID associated with the recommended solution.
Solution	A description for the solution.
Tenable UUID	The Tenable UUID, if applicable. A Tenable UUID uniquely identifies: • Agent-detected assets that may share a common IP address. • Tenable One OT Exposure assets that may not have an IP address. For more information, see Tenable One OT Exposure Instances.
DNS	The DNS name of the device, if known.
IP Address	The IP address for the device.
OS	The operating system running on the device.
CVEs	The number of unique CVEs associated with vulnerabilities on the affected host that are addressed by the solution.
CVE Instances	The total number of CVE instances associated with vulnerabilities on the affected host that are addressed by 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.
OS CPE	The operating system common platform enumeration (CPE) name of the device.
Repository	The name of the repository that stores the device's scan data.
MAC	The MAC address of the device, if known.
NetBIOS	The NetBIOS name of the device, if known.
Vulnerabilities	The total number of vulnerability instances on the affected host addressed by 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.
Vulnerability Percentage	The number of vulnerability instances on the affected host addressed by the solution as a percentage of total vulnerability instances. **Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.
Score	The sum of the weighted CVSS score across vulnerability instances on the affected host addressed by the solution. **Note:** Tenable Security Center Director uses either CVSSv2 or CVSSv3 to assess the severity of vulnerabilities, depending on your configuration. For more information, see Organizations. **Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and

	protocol.
Risk Reduction	The percent you would reduce your risk across all solutions and affected hosts by addressing the vulnerabilities on this affected host associated with the solution. Tenable Security Center Director calculates the risk reduction percentage by dividing the total CVSS score of the vulnerabilities on the affected host addressed by the solution by the total CVSS score of all of the vulnerabilities on your network. **Note:** Tenable Security Center Director uses either CVSSv2 or CVSSv3 to assess the severity of vulnerabilities, depending on your configuration. For more information, see Organizations.
MS Bulletins	The number of unique MS Bulletins associated with vulnerabilities on the affected host that are addressed by the solution.
MS Bulletin Instances	The total number of vulnerabilities with associated MS Bulletins on the affected host that are addressed by the solution.
VPR	The highest VPR of all vulnerabilities on the affected host that are addressed by the solution. If no VPR is available, the column is blank.
CVSS v3	The highest CVSSv3 score of all vulnerabilities on the affected host that are addressed by the solution. If only a CVSSv2 score is available, the column is blank.

6. Click **Download**.

Tenable Security Center Director exports the list of hosts affected by the solution.

Vulnerability Analysis

The **Vulnerabilities** 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 Security Center 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 Security Center 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 recast, accepted, or previously mitigated vulnerabilities.

Mitigated Vulnerabilities

The mitigated database contains vulnerabilities that Tenable Security Center 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 appear 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.

CVSS vs. VPR

Tenable uses CVSS scores and a dynamic Tenable-calculated Vulnerability Priority Rating (VPR) to quantify the risk and urgency of a vulnerability.

> **Note:** When you view these metrics on an analysis page organized by plugin (for example, the **Vulnerabilities** page), the metrics represent the highest value assigned or calculated for a vulnerability associated with the plugin.

CVSS

Tenable uses and displays third-party Common Vulnerability Scoring System (CVSS) values retrieved from the National Vulnerability Database (NVD) to describe risk associated with vulnerabilities.

Tenable assigns all vulnerabilities a severity (**Info**, **Low**, **Medium**, **High**, or **Critical**) based on the vulnerability's static CVSS score (the CVSS version depends on your configuration). For more information, see Organizations.

Tenable Security Center analysis pages provide summary information about vulnerabilities using the following CVSS categories.

Caution: If the most severe CVE is a denial of service vulnerability, the overall score is based on the highest non-denial of service vulnerability. This nuance isn't something many people know, and is a frequent source of confusion.

Severity	CVSSv2 Range	CVSSv3 Range
Critical	The plugin's highest vulnerability CVSSv2 score is 10.0.	The plugin's highest vulnerability CVSSv3 score is between 9.0 and 10.0.
High	The plugin's highest vulnerability CVSSv2 score is between 7.0 and 9.9.	The plugin's highest vulnerability CVSSv3 score is between 7.0 and 8.9.
Medium	The plugin's highest vulnerability CVSSv2 score is between 4.0 and 6.9.	The plugin's highest vulnerability CVSSv3 score is between 4.0 and 6.9.
Low	The plugin's highest vulnerability CVSSv2 score is between 0.1 and 3.9.	The plugin's highest vulnerability CVSSv3 score is between 0.1 and 3.9.
Info	The plugin's highest vulnerability CVSSv2 score is 0. - or - The plugin does not search for vulnerabilities.	The plugin's highest vulnerability CVSSv3 score is 0. - or - The plugin does not search for vulnerabilities.

Vulnerability Priority Rating

Tenable calculates a dynamic VPR for most vulnerabilities. The VPR is a dynamic companion to the data provided by the vulnerability's CVSS score, since Tenable updates the VPR to reflect the

current threat landscape. VPR values range from 0.1-10.0, with a higher value representing a higher likelihood of exploit.

VPR Category	VPR Range
Critical	9.0 to 10.0
High	7.0 to 8.9
Medium	4.0 to 6.9
Low	0.1 to 3.9

Note: Vulnerabilities without CVEs (for example, 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 Security Center provides new and updated VPR values through the Tenable Security Center 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

Some key drivers that you can view to explain a vulnerability's VPR include, but are not limited to:

Note: Tenable does not customize these values for your organization; VPR key drivers reflect a vulnerability's global threat landscape.

Key Driver	Description
Vulnerability Age	The number of days since the National Vulnerability Database (NVD) published the vulnerability.
CVSSv3 Impact Score	The NVD-provided CVSSv3 impact score for the vulnerability. If the NVD did not provide a score, Tenable Security Center displays a Tenable-predicted score.
Exploit Code Maturity	The relative maturity of a possible exploit for the vulnerability based on the existence, sophistication, and prevalence of exploit intelligence from internal and external sources (e.g., Reversinglabs, Exploit-db, Metasploit, etc.). The possible values (**High**, **Functional**, **PoC**, or **Unproven**) parallel the CVSS Exploit Code Maturity categories.
Product Coverage	The relative number of unique products affected by the vulnerability: **Low**, **Medium**, **High**, or **Very High**.
Threat Sources	A list of all sources (e.g., social media channels, the dark web, etc.) where threat events related to this vulnerability occurred. If the system did not observe a related threat event in the past 28 days, the system displays **No recorded events**.
Threat Intensity	The relative intensity based on the number and frequency of recently observed threat events related to this vulnerability: **Very Low**, **Low**, **Medium**, **High**, or **Very High**.
Threat Recency	The number of days (0-180) since a threat event occurred for the vulnerability.

Threat Event Examples

Common threat events include:

- An exploit of the vulnerability
- A posting of the vulnerability exploit code in a public repository
- A discussion of the vulnerability in mainstream media
- Security research about the vulnerability
- A discussion of the vulnerability on social media channels
- A discussion of the vulnerability on the dark web and underground
- A discussion of the vulnerability on hacker forums

Manage Vulnerabilities

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

View Cumulative or Mitigated Vulnerabilities

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 Security Center Director via the user interface.
2. Click **Analysis** > **Vulnerabilities**.

   The **Vulnerabilities** page appears.
3. In the upper-right corner, click **Cumulative** or **Mitigated**.

   The page updates to display data from the mitigated or cumulative vulnerability database.

View Vulnerabilities by Host

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 Security Center Director via the user interface.
2. Click **Analysis** > **Vulnerabilities**.

   The **Vulnerabilities** 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. To customize the table, see Interact with a Customizable Table.
6. To view details of a vulnerability instance:
   a. Click the row for the vulnerability instance for which you want to view the details.

      The **Vulnerability List** tool appears, filtered by the vulnerability instance you selected.

      In this tool, you can:

Options	Actions
Jump to Vulnerability Detail	View the **Vulnerability Detail List** page. This page displays the synopsis, description, solution, and the plugin output of the vulnerability.
Export	Export data as a .csv or a .pdf file, as described in Export Vulnerability Data.
Save	• **Save Query** – Save a query, as described in Add or Save a Query. • **Save Asset** – Save an asset, as described in Asset Tags.
More	• **Open Ticket** – Open a ticket, as described in Open a Ticket. • **Set as Default View** – Set this view as your default view.

Cumulative	Switch between viewing cumulative vulnerabilities or mitigated vulnerabilities, as described in View Cumulative or Mitigated Vulnerabilities.
Mitigated	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.

7. To view the host details of an instance:
    a. Click the **IP Address** link.

    The **System Information** pane appears. For more information, see View Host Details.

View Vulnerabilities by Plugin

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 Security Center Director via the user interface.
2. Click **Analysis** > **Vulnerabilities**.

The **Vulnerabilities** page appears.

3. In the drop-down box, click **Vulnerability Summary**.

   The **Vulnerability Summary** tool appears.

   In this tool, you can:

Options	Actions
Jump to Vulnerability Detail	View the **Vulnerability Detail List** page. This page displays the synopsis, description, solution, and the plugin output of the vulnerability.
Export	Export data as a .csv or a .pdf file, as described in Export Vulnerability Data.
Save	• **Save Query**: Save a query, as described in Add or Save a Query. • **Save Asset**: Save an asset, as described in Asset Tags.
More	• **Open Ticket**: Open a ticket, as described in Open a Ticket. • **Set as Default View**: Set this view as your default view.
Cumulative	Switch between viewing cumulative vulnerabilities or mitigated vulnerabilities, as described in View Cumulative or Mitigated Vulnerabilities.
Mitigated	Switch between viewing cumulative vulnerabilities or mitigated vulnerabilities, as described in View Cumulative or Mitigated Vulnerabilities.
Table	Customize the table, as described in Interact with a Customizable 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	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:

Options	Actions
Jump to Vulnerability Detail	View the **Vulnerability Detail List** page. This page displays the synopsis, description, solution, and the plugin output of the vulnerability.
Export	Export data as a .csv or a .pdf file, as described in Export Vulnerability Data.
Save	• **Save Query** – Save a query, as described in Add or Save a Query. • **Save Asset** – Save an asset, as described in Asset Tags.
More	• **Open Ticket** – Open a ticket, as described in Open a Ticket. • **Set as Default View** – Set this view as your default view.
Cumulative	Switch between viewing cumulative vulnerabilities or mitigated

	vulnerabilities, as described in View Cumulative or Mitigated Vulnerabilities.
Mitigated	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.

BOD 26-04 and SSVC columns

If your organization uses CISA BOD 26-04, the **Vulnerability List** tool includes the following columns. You cannot sort the table by these columns.

Column	Description
CISA SLA	The BOD 26-04 remediation tier for the vulnerability: **3-day + triage**, **3-day**, **14-day**, **60-day**, **Fix on upgrade**, or **Undetermined**. Tenable Security Center determines the tier from the CISA SSVC signals for the plugin and whether the affected asset is internet-facing. This column appears only when BOD 26-04 is enabled for your

Column	Description
	organization. For more information, see Edit an Organization.
SLA Time Left	The time remaining before the remediation due date. The due date is the date and time the vulnerability was first found plus the number of days for its tier. A negative value means the vulnerability is overdue. Vulnerabilities in the **Fix on upgrade** and **Undetermined** tiers have no due date. This column appears only when BOD 26-04 is enabled for your organization. For more information, see Edit an Organization.
SSVC Signals	The CISA SSVC signals for the plugin: whether the vulnerability is in the CISA Known Exploited Vulnerabilities (KEV) catalog, whether exploitation is automatable (**Auto: Yes** or **Auto: No**), and the technical impact (**Impact: Partial** or **Impact: Total**).
SSVC CVE Driver	The CVE that drives the SSVC signals for the plugin.

Informational plugins do not display values in these columns. For information about filtering on these values, see Vulnerability Analysis Filter Components

View Vulnerability Instance Details

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 Security Center Director via the user interface.
2. Click **Analysis** > **Vulnerabilities**.

   The **Vulnerabilities** page appears.
3. In the drop-down box, click **Vulnerability Detail List**.

   The **Vulnerability Detail List** tool appears.

   In this tool, you can:

Section	Actions
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 this view as your default view. • Switch between viewing cumulative vulnerabilities or mitigated vulnerabilities, as described in View Cumulative or Mitigated Vulnerabilities.
arrows	Click the arrows to view other vulnerability instances related to the plugin.
toolbar	• 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.
Plugin Output	The output generated by the plugin. **Note:** Tenable Nessus scanners may occasionally report findings from plugin 19506 multiple times per host. Tenable Security Center Director reports all of the plugin output from a host, including different findings for the same plugin ID. These findings appear as multiple entries in the **Vulnerability Detail List** tool.
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 (for example, CVSS score, VPR, and EPSS) about the risk associated with the vulnerability.
CISA BOD 26-04 or SSVC	View the Stakeholder-Specific Vulnerability Categorization (SSVC) information for the vulnerability instance. The section title depends on whether BOD 26-04 is enabled for your organization. For more information, see Edit an Organization. • If BOD 26-04 is enabled for your organization, the section is titled **CISA BOD 26-04**. It includes the SSVC information, the CISA SLA tier, the due date, and the time left. If Tenable Security Center cannot assign a tier, this section explains why. • If BOD 26-04 is not enabled for your organization, the section is

	titled **SSVC**. It includes whether the vulnerability is on the CISA KEV list, whether exploitation is automatable, the technical impact, the SSVC CVE driver, and the SSVC role and version.
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 CVSS 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.

Export Vulnerability Data

You can export data from the **Vulnerabilities** page as a `.csv` or a `.pdf` file.

To export data from the Vulnerabilities page:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Analysis** > **Vulnerabilities**.

   The **Vulnerabilities** page appears.
3. In the **Export** drop-down box, click **Export** > **Export as CSV** or **Export as PDF**.

   Note: If the record count (rows displayed) of any CSV export is greater than 1,000, Tenable Security Center 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.
4. Select or clear the check boxes to indicate which columns you want to appear in the exported file.

5. Click **Submit**.

   Tenable Security Center Director exports the vulnerability data.

View Host Details

> **Required Tenable Security Center 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 Security Center Director via the user interface.
2. Click **Analysis** > **Vulnerabilities**.

   The **Vulnerabilities** page appears.
3. In the drop-down box, click **Vulnerability List**.

   The **Vulnerability List** tool appears.
4. In the **IP Address** column, click the IP address link 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.

Section	Actions
System Information	View information about the host system. • **IP Address** – The host's IP address, if available. • **UUID** – The host's UUID, if available. • **NetBIOS Name** – The host's NetBIOS name, if available.

	• **DNS Name** – The host's DNS name, if available. • **MAC Address** – The host's MAC address, if available. • **OS** – The operating system running on the host, if available. • **CPE** – The host's application common platform enumeration (CPE). • **Score** – The cumulative score for all vulnerability instances on the host. For more information about vulnerability scoring, see CVSS vs. VPR. **Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol. • **Repository** – The repository that contains vulnerability data associated with the host. • **Last Scan** – The date and time Tenable Security Center last scanned the host. • **Passive Data** – Indicates whether a passive scan detected the vulnerability. • **Compliance Data** – Indicates whether the scan that detected the vulnerability included compliance plugins.
Vulnerabilities	View the number of vulnerabilities on the host, organized by severity category. For more information, see CVSS vs. VPR.
Links	• 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.
Assets	View the asset lists containing the asset. For more information, see Asset Tags.

To view host details from the **Host Assets** page:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Assets** > **Host Assets**.

   The **Host Assets** page appears.
3. Click the row for the host.

   The **Host Asset Details** page appears.

Section	Action
Host Information	View general information about the host. • **Name** – The name of the host. • **System Type** – The host's device type, as determined by plugin 54615. • **Operating System** – The operating system running on the host, if available. • **IP Addresses** – The host's IP address, if available. • **MAC Addresses** – The host's MAC address, if available. • **Asset ID** – The ID of the host. • **Repository** – The repository that contains vulnerability data associated with the host.
Asset Criticality	(Requires Tenable Security Center+ license) View the host's ACR and details about modifications to the ACR.

Section	Action
Rating	• **Overwrite Reasoning** – The justification for overwriting the host's ACR. • **Notes** – Notes associated with overwriting the host's ACR. • **Overwritten By** – The user that overwrote the host's ACR. • **ACR By Key Drivers** – The key drivers used to calculate the host's ACR. For more information, see Asset Criticality Rating and ACR Key Drivers in the *Tenable One Vulnerability Management User Guide*. **Tip:** To edit the host's ACR, log in to the managed Tenable Security Center instance that contains the host's data. For more information, see Edit an ACR Manually in the *Tenable Security Center User Guide*.
Scan Information	View scan information related to the host. • **First Seen** – The date and time Tenable Security Center first detected the host on your network. • **Last Seen** – The date and time last Tenable Security Center detected the host on your network. • **Source** – The type of scan that discovered the host on your network: **Tenable Nessus Scan**, **Tenable Network Monitor**, **Agent Scan**, or **Tenable One OT Exposure Scan**.
Findings tab	View the vulnerabilities detected on the host. For more information, see CVSS vs. VPR. Customize the table, as described in Interact with a Customizable Table.

Section	Action
Installed Software tab	View the software packages installed on the host, if available. Customize the table, as described in Interact with a Customizable Table.

View Plugin Details

Required Tenable Security Center 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 Security Center Director via the user interface.
2. Click **Analysis** > **Vulnerabilities**.

   The **Vulnerabilities** page appears.
3. In the drop-down box, click **Vulnerability Summary**.

   The **Vulnerability Summary** tool appears.
4. To customize the table, see Interact with a Customizable Table.
5. In the **Plugin ID** column, click the plugin ID to view plugin details for a specific plugin.

   The **Plugin Details** panel appears.

   In this panel, you can:

Section	Actions
Description	View information about the plugin, vulnerability instance, and affected assets.
Solution	View the Tenable-recommended action to remediate the vulnerability.
Vulnerability Priority Rating (VPR) Key Drivers	View the key drivers Tenable used to calculate the vulnerability VPR. For more information, see CVSS vs. VPR.
CVE and **BID**	View related links to the CVE and BID materials about the vulnerability.
Cross-References	View related documentation for the vulnerability.
See Also	View related links about the plugin or vulnerability.

Vulnerability Analysis Tools

On the **Vulnerabilities** 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.

Analysis Tool	Description
Asset Summary	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.

Analysis Tool	Description
	You can click a count to view the **IP Summary** tool, filtered by the asset list you selected.
CCE Summary	This displays a summary of hosts which have Common Configuration Enumeration (CCE) vulnerabilities. You can click a count to view the **Vulnerability Summary** tool, filtered by the CCE vulnerability you selected.
Class A Summary **Class B Summary** **Class C Summary**	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 **Class A** or **Class B** row to view the **Class B** or **Class C** tool, filtered by the asset list you selected. You can click a **Class C** row to view the **IP Summary** tool, filtered by the asset list you selected.
CVE Summary	This view groups vulnerabilities based on their CVE ID, severity, and vulnerability count.
DNS Name Summary	Tenable Security Center 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. You can click a DNS name to view the **Vulnerability List** tool, filtered by the DNS name you selected.

Analysis Tool	Description
IAVM Summary	This view groups vulnerabilities based on their IAVM ID, severity, and vulnerability count.
IP Summary	Summarizes host information, organized by IP address/agent ID. You can click the **IP Address** to view host details, as described in View Host Details. For more information, see View Vulnerabilities by Host.
List Mail Clients	Tenable Security Center uses Tenable Network Monitor to determine a unique list of email clients. The list contains the email client name, count of detections, and the detection method. You can click a count to view the **IP Summary** tool, filtered by the email client you selected.
List OS	Tenable Security Center understands both actively and passively fingerprinted operating systems. This tool lists what has been discovered. The method (active, passive, or event) of discovery is also indicated. You can click a count to view the **IP Summary** tool, filtered by operating system.
List Services	Tenable Security Center processes information from scans and creates a summary of unique services discovered. The service discovered, count of hosts, and detection method are listed. You can click a service to view the **IP Summary** tool, filtered by the service you selected.
List Software	Tenable Security Center processes information from scans and creates a summary of unique software packages discovered. The software name,

Analysis Tool	Description
	count of hosts, and detection method are listed. You can click a software name to view the **IP Summary** tool, filtered by the software you selected.
List SSH Servers	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. **Tip:** Not all SSH servers run on port 22. Do not be surprised if you encounter SSH servers running on unexpected ports. You can click a count to view the **IP Summary** tool, filtered by the SSH server you selected.
List Web Clients	Tenable Security Center understands Tenable Network Monitor 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 **IP Summary** tool, filtered by the web client you selected.
List Web Servers	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 **IP Summary** tool, filtered by the web server you selected.

Analysis Tool	Description
MS Bulletin Summary	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.
Plugin Family Summary	This tool charts the Nessus, Tenable Network Monitor, 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 **Vulnerability List** tool, filtered by the plugin family you selected.
Port Summary	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 **IP Summary** tool, filtered by the port you selected.
Protocol Summary	This tool summarizes the detected IP protocols such as TCP, UDP, and ICMP. The tool also breaks out the counts for each protocol's severity levels. You can click a count to view the **IP Summary** tool, filtered by the count you selected.
Remediation Summary	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: • **Risk Reduction** – The percent you would reduce your risk by

Analysis Tool	Description
	addressing the vulnerability in the solution. Tenable Security Center 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 unique hosts that would be affected by performing the remediation action. • **Vulnerabilities** – The count of vulnerabilities (Tenable Nessus plugins) that would be remediated by performing the remediation action. • **Score** – This is calculated by adding up the score for each vulnerability that would be remediated by performing the remediation action. • **CVE** – The number of distinct CVEs that would be remediated by performing the remediation action. • **MS Bulletin** – The number of unique MS Bulletins that would be remediated by performing the remediation action. • **Vulnerability %** – The count of vulnerabilities (Tenable Nessus plugins) that would be remediated by performing the remediation action over the total vulnerability count returned by the query as a percentage.
Severity Summary	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 **Vulnerability Summary** tool, filtered by the severity you selected.
User	This displays a list of the users who are assigned responsibility for the

Analysis Tool	Description
Responsibility Summary	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 Security Center populates this list after you assign an asset to a user account.
Vulnerability Detail List	Displays the details for a specific vulnerability instance 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. 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. For more information, see View Vulnerability Instance Details.
Vulnerability List	Displays a table of all vulnerability instances found on your network, organized by plugin ID. **Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol. For more information, see View Vulnerabilities by Plugin.
Vulnerability Summary	Displays a table of all plugins associated with vulnerabilities on your network, organized by plugin ID. For more information, see View Vulnerabilities by Plugin.

Vulnerability Analysis Filter Components

For general information about using filters, see Filters.

Filter Component	Availability	Description
Accept Risk	Cumulative View	Displays 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.
Address	All	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 show vulnerability data from the specified networks. You can enter addresses in a comma-separated list or on separate lines.
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 One OT Exposure assets that may not have an IP address. For more information, see Tenable One OT Exposure 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

Filter Component	Availability	Description
		more than one asset contains the systems from the primary asset (i.e., there is an intersect between the asset lists), those assets are displayed as well. **Tip:** Use NOT, OR, and AND operators to exclude unwanted assets from the view.
Asset Exposure Score (AES)	All	(Requires Tenable Security Center+ license) Filters for hosts within the specified AES range, between 0 and 1000. For more information, see Asset Exposure Score in the *Tenable One Vulnerability Management User Guide*.
AES Severity	All	(Requires Tenable Security Center+ license) Filters for hosts with the specified AES severity. For more information, see Asset Exposure Score in the *Tenable One Vulnerability Management User Guide*.
Audit File	All	Filters vulnerabilities by plugin IDs associated with the audit file used to perform a scan.
BOD 26-04 Internet Facing	All	Displays vulnerabilities based on whether the affected asset is designated as internet-facing for CISA BOD 26-04. Select **Yes** or **No**. Vulnerabilities on assets with an unknown exposure match neither option. This filter appears only when BOD 26-04 is enabled for your organization. For more information, see Edit an Organization.

Filter Component	Availability	Description
CCE ID	All	Displays results matching the entered CCE ID.
CISA KEV	All	Displays vulnerabilities based on whether the vulnerability is in the CISA Known Exploited Vulnerabilities (KEV) catalog. Select **Yes** or **No**.
CISA SLA	All	Displays vulnerabilities based on their BOD 26-04 remediation tier. Select one or more of the following tiers: **3-day + triage**, **3-day**, **14-day**, **60-day**, **Fix on upgrade**, or **Undetermined**. Filtering on **Undetermined** returns vulnerabilities that BOD 26-04 applies to but that Tenable Security Center cannot yet assign a remediation timeline to. This happens when no CISA SSVC decision data (KEV status, exploit automation, technical impact) is available for the plugin, or when the internet exposure of the asset is not yet known. Informational findings whose plugin does not reference a CVE are outside BOD 26-04, which identifies vulnerabilities by CVE ID. These findings have no CISA SLA, and no CISA SLA filter returns them. Informational findings whose plugin references a CVE are graded like any other finding. This filter appears only when BOD 26-04 is enabled for your organization. For more information, see Edit an Organization.
CVE ID	All	Displays vulnerabilities based on one or more CVE IDs.

Filter Component	Availability	Description
		Type multiple IDs as a comma-separated list (e.g., **CVE-2011-3348,CVE-2011-3268,CVE-2011-3267**).
CVSS v2 Score	All	Displays vulnerabilities within the chosen Common Vulnerability Scoring System version 2 (CVSS v2) score range.
CVSS v2 Vector	All	Filters results based on a search against the CVSS v2 vector information.
CVSS v3 Score	All	Displays vulnerabilities within the chosen CVSS v3 score range.
CVSS v3 Vector	All	Filters results based on a search against the CVSS v3 vector information.
CVSS v4 Score	All	Displays vulnerabilities within the chosen CVSS v4 score range.
CVSS v4 Supplemental	All	Filters results based on a search against the CVSS v4 supplemental information.
CVSS v4 Threat Score	All	Displays vulnerabilities within the chosen CVSS v4 threat score range.
CVSS v4 Threat Vector	All	Filters results based on a search against the CVSS v4 threat vector information.
CVSS v4 Vector	All	Filters results based on a search against the CVSS v4 vector information.
Cross	All	Filters results based on a search against the cross

Filter Component	Availability	Description
References		reference information in a vulnerability. **Note:** For agent-based audit results, cross reference data is only available if both of the following are true: the audit file has been added to Tenable Security Center, and either a scan has been initiated from Tenable Security Center using that audit, or the audit has been used as a filter in the Vulnerability Analysis tool. If these conditions are not met, the **Cross References** filter returns no results for agent audit data. This is expected behavior.
Data Format	All	Displays results matching the specified data type: **IPv4**, **IPv6**, or **Agent**.
DNS Name	All	This filter specifies a DNS name to limit the viewed vulnerabilities. For example, entering host.example.com limits any of the web tools to only show vulnerability data from that DNS name.
Exploit Prediction Scoring System (EPSS)	All	Filters results by the EPSS score, which predicts how likely a vulnerability is to be exploited.
Exploit Available	All	If set to yes, displays only vulnerabilities for which a known public exploit exists.
Exploit Frameworks	All	When set, the text option can be equal to or contain the text entered in the option.
IAVM ID	All	Displays vulnerabilities based on one or more IVAM IDs. Type multiple IDs as a comma-separated list (e.g.,

Filter Component	Availability	Description
		2011-A-0005,2011-A-0007,2012-A-0004).
MS Bulletin ID	All	Displays vulnerabilities based on one or more Microsoft Bulletin IDs. Type multiple IDs as a comma-separated list (e.g., *MS10-012,MS10-054,MS11-020*).
Mitigated	All	Displays vulnerabilities for a specific mitigation status: • **Previously Mitigated** – the vulnerability was previously mitigated but it reappeared in a scan and is currently vulnerable • **Never Mitigated** – the vulnerability is currently vulnerable and has never been mitigated For more information about mitigation, see Mitigated Vulnerabilities.
Nessus Web Tests	All	Displays vulnerabilities that are detected by a scan with Nessus Web Tests enabled in the scan policy.
NetBIOS Name	All	Displays vulnerabilities that match the specified NetBIOS name. In the drop-down, select **Exact Match**, **Contains**, or **Regex Match**. **Regex Match** is based on Perl-compatible regular expressions (PCRE). **Note**: You cannot filter NetBIOS Name by UNKNOWN. The NetBIOS workgroup is labeled UNKNOWN when a workgroup or domain cannot be detected.
Output Assets	Asset	This filter displays only the desired asset list systems.

Filter Component	Availability	Description
	Summary Analysis Tool	
Patch Published	All	Some plugins contain information about when a patch was published for a vulnerability. This filter allows the user to search based on when a vulnerability's patch became available: • **None** (displays vulnerabilities that do not have a patch available) • **Within the last day** • **Within the last 7 days** • **Within the last 30 days** • **More than 7 days ago** • **More than 30 days ago** • **Current Month** • **Last Month** • **Current Quarter** (during the current calendar year quarter) • **Last Quarter** (during the previous calendar year quarter) • **Current Year** • **Last Year** • **Custom Range** (during a specific range you specify) • **Explicit** (at a specific time you specify)

Filter Component	Availability	Description
Plugin Family	All	This filter chooses a Nessus or Tenable Network Monitor 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 (>=) and less than or equal to (<=).
Plugin Modified	All	Tenable plugins contain information about when a plugin was last modified. This filter allows users to search based on when a particular plugin was modified: • **Within the last day** • **Within the last 7 days** • **Within the last 30 days** • **More than 7 days ago** • **More than 30 days ago** • **Current Month** • **Last Month** • **Current Quarter** (during the current calendar year quarter) • **Last Quarter** (during the previous calendar year quarter) • **Current Year** • **Last Year** • **Custom Range** (during a specific range you specify)

Filter Component	Availability	Description
		• **Explicit** (at a specific time you specify)
Plugin Name	All	Using the **Contains** option, type all or a portion of the actual plugin name. For example, entering **MS08-067** in the plugin name filter displays vulnerabilities using the plugin named **MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)**. Similarly, entering the string **uncredentialed** displays a list of vulnerabilities with that string in the plugin name. Use the **Regex Match** option to filter plugin names based on Perl-compatible regular expressions (PCRE).
Plugin Output	All	Displays vulnerabilities containing the entered text (e.g., php 5.3) or regex search term.
Plugin Published	All	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: • **Within the last day** • **Within the last 7 days** • **Within the last 30 days** • **More than 7 days ago** • **More than 30 days ago** • **Current Month** • **Last Month** • **Current Quarter** (during the current calendar year

Filter Component	Availability	Description
		quarter) • **Last Quarter** (during the previous calendar year quarter) • **Current Year** • **Last Year** • **Custom Range** (during a specific range you specify) • **Explicit** (at a specific time you specify)
Plugin Type	All	Select whether to view all plugin types or passive, active, event, or compliance vulnerabilities.
Port	All	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 than** or **less than** filters, only one port may be used. **Note:** All host-based vulnerability checks are reported with a port of 0 (zero).
Protocol	All	This filter provides boxes to select TCP, UDP, or ICMP-based vulnerabilities.
Recast Risk	Cumulative View	Displays 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.

Filter Component	Availability	Description
Repositories	All	Displays vulnerabilities from the chosen repositories.
STIG Severity	All	Displays vulnerabilities with the chosen STIG severity in the plugins database.
Scan Accuracy	All	Displays vulnerabilities that are detected by scans with the chosen scan accuracy: • **Not Paranoid** – the vulnerability was detected by a scan with the scan accuracy set to Not Paranoid in the scan policy. • **Paranoid** – the vulnerability was detected by a scan with the scan accuracy set to Paranoid in the scan policy.
Scan Policy Plugins	All	Displays vulnerabilities found by the currently enabled plugins in the scan policy. For more information, see Plugins Options.
Security End of Life Date	All	When available, Tenable plugins contain information about software end of life dates. This filter allows users to search based on when a particular software is end of life: • **Within the last day** • **Within the last 7 days** • **Within the last 30 days** • **More than 7 days ago** • **More than 30 days ago** • **Current Month**

Filter Component	Availability	Description
		• **Last Month** • **Current Quarter** (during the current calendar year quarter) • **Last Quarter** (during the previous calendar year quarter) • **Current Year** • **Last Year** • **Custom Range** (during a specific range you specify) • **Explicit** (at a specific time you specify)
Severity	All	Displays vulnerabilities with the selected severity. For more information, see CVSS vs. VPR.
SLA Time Left	All	Displays vulnerabilities based on the time remaining before their BOD 26-04 remediation due date. Select **Overdue**, a number of days (3, 7, 14, 30, or 60) in which the vulnerability is due, or enter a custom date range. This filter appears only when BOD 26-04 is enabled for your organization. For more information, see Edit an Organization.
SSVC CVE Driver	All	Displays vulnerabilities based on the CVE that drives the SSVC signals for the plugin. Type a CVE ID.
SSVC: Automatable	All	Displays vulnerabilities based on whether the CISA SSVC assessment considers exploitation of the vulnerability automatable. Select **Yes** or **No**.

Filter Component	Availability	Description
SSVC: Technical Impact	All	Displays vulnerabilities based on the technical impact in the CISA SSVC assessment. Select **Partial** or **Total**.
Thorough Tests	All	Displays vulnerabilities that are detected by scans with Thorough Tests enabled in the scan policy.
Users	All	Allows selection of one or more users who are responsible for the vulnerabilities.
Vulnerability Discovered	All	Tenable Security Center tracks when each vulnerability was first discovered. This filter allows you to see when vulnerabilities were discovered: • **Within the last day** • **Within the last 7 days** • **Within the last 30 days** • **More than 7 days ago** • **More than 30 days ago** • **Current Month** • **Last Month** • **Current Quarter** (during the current calendar year quarter) • **Last Quarter** (during the previous calendar year quarter) • **Current Year** • **Last Year** • **Custom Range** (during a specific range you specify)

Filter Component	Availability	Description
		• **Explicit** (at a specific time you specify) **Note:** The discovery date is based on when the vulnerability was first imported into Tenable Security Center or updated to the resurfaced date. For Tenable Network Monitor, this date does not match the exact vulnerability discovery time as there is normally a lag between the time that Tenable Network Monitor discovers a vulnerability and the import occurs. **Note:** 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.
Vulnerability Last Observed	Cumulative View	This filter allows the user to see when the vulnerability was last observed by Tenable Nessus or Tenable Network Monitor: • **Within the last day** • **Within the last 7 days** • **Within the last 30 days** • **More than 7 days ago** • **More than 30 days ago** • **Current Month** • **Last Month** • **Current Quarter** (during the current calendar year quarter) • **Last Quarter** (during the previous calendar year quarter)

Filter Component	Availability	Description
		• **Current Year** • **Last Year** • **Custom Range** (during a specific range you specify) • **Explicit** (at a specific time you specify) **Note:** The observation date is based on when the vulnerability was most recently imported into Tenable Security Center. For Tenable Network Monitor, this date does not match the exact vulnerability discovery as there is normally a lag between the time that Tenable Network Monitor discovers a vulnerability and the import occurs.
Vulnerability Mitigated	Mitigated View	This filter allows the user to filter results based on when the vulnerability was mitigated: • **Within the last day** • **Within the last 7 days** • **Within the last 30 days** • **More than 7 days ago** • **More than 30 days ago** • **Current Month** • **Last Month** • **Current Quarter** (during the current calendar year quarter) • **Last Quarter** (during the previous calendar year quarter) • **Current Year**

Filter Component	Availability	Description
		• **Last Year** • **Custom Range** (during a specific range you specify) • **Explicit** (at a specific time you specify)
Vulnerability Priority Rating (VPR)	All	Displays vulnerabilities within the chosen VPR range. For more information, see CVSS vs. VPR. **Tip:** The **Vulnerabilities** page displays vulnerabilities by plugin. The VPR that appears is the highest VPR of all the vulnerabilities associated with that plugin.
Vulnerability Published	All	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: • **All** • **Within the last day** • **Within the last 7 days** • **Within the last 30 days** • **More than 7 days ago** • **More than 30 days ago** • **Current Month** • **Last Month** • **Current Quarter** (during the current calendar year quarter) • **Last Quarter** (during the previous calendar year

Filter Component	Availability	Description
		quarter) • **Current Year** • **Last Year** • **Custom Range** (during a specific range you specify) • **Explicit** (at a specific time you specify)
Web App Scanning	All	**Required Additional License:** Tenable One Web App Scanning **Required Tenable Nessus Version:** 10.6.1 or later Select whether to display web app scan results in the list: • **Exclude Web App Results** - do not display web app scan results in the list of vulnerabilities. • **Include Web App Results** - include web app scan results in the list of vulnerabilities. • **Only Web App Results** - filter the list to display only web app scans results.
Web App URL	All	**Required Additional License:** Tenable One Web App Scanning **Required Tenable Nessus Version:** 10.6.1 or later The URL for the discovered web application associated with the vulnerability.

Vulnerability Intelligence

Required License: Tenable Security Center Director Subscription or Tenable Security Center Director Perpetual with Vulnerability Intelligence add-on

Note: If you have more than 100,000 assets or a non-rpm installation, you must connect an external PostgreSQL server to use Vulnerability Intelligence.

In the **Vulnerability Intelligence** section, you can review all vulnerabilities known to Tenable without leaving Tenable Security Center Director. The vulnerabilities come from Tenable's database, which draws on sources such as internal expertise, vendor advisories, the GitHub Advisory Database, and the National Vulnerability Database (NVD).

The **Vulnerability Intelligence** section also holds curated categories that blend known risk indicators with insights from the Tenable Research Team to surface the most crucial vulnerabilities.

Once you have chosen which vulnerabilities to focus on, you compare them to your own findings and build a list to take action on. To do this, use the query builder to refine the results and save your searches to re-use or share.

The following topics explain how to use the tools in the **Vulnerability Intelligence** section to: 1) search Tenable's vulnerability database, 2) view vulnerability profiles, and 3) identify your exposure when compared to known vulnerabilities.

Search Known Vulnerabilities

On the **Vulnerability Intelligence Overview** page, you can search all vulnerabilities known to Tenable by *Common Vulnerabilities and Exposures* (CVE) ID.

To search for a vulnerability:

1. In the left navigation, click **Vulnerability Intelligence**.

   The **Vulnerability Intelligence Overview** page appears.

2. In the header, in the search box, type a complete or partial search (for example, *CVE-2014-0160* or *2014*).
3. Press the **Enter** key.
4. In the list of results, click a vulnerability.

   The **Vulnerability Profile** page appears.

View Vulnerability Profiles

On the **Vulnerability Intelligence Overview** page, when you click a search result or a row in the **CVEs** tab, the **Vulnerability Profile** page appears.

The **Vulnerability Profile** page breaks down a single vulnerability in detail and includes an event timeline, your affected assets and products, the sources, and metrics such as risk profile and severity.

The **Vulnerability Profile** page has four sections.

In this Section	You Can...
Vulnerability Information	View the Common Vulnerability Scoring System (CVSS), Vulnerability Priority Rating (VPR), and Exploit Prediction Scoring System (EPSS) scores. In tabs, review an event timeline, VPR and EPSS trends, identifying plugins, all known products affected, and a summary.
How Does This Affect Me?	View affected assets and products in your environment and build queries to refine the results.
Sources	View contextual intelligence such as security advisories on the external websites where they appear.
Vulnerability Metrics	In a right-hand pane, review metrics broken down by general information, risk profile, severity, and plugin coverage.

Vulnerability Information

On the **Vulnerability Profile** page, the **Vulnerability Information** section provides a short summary along the vulnerability's Vulnerability Priority Rating (VPR), Common Vulnerability Scoring System (CVSS), and Exploit Prediction Scoring System (EPSS) scores.

It also contains four tabs, within which you can view an event timeline, VPR and EPSS widgets, plugin details, known affected products, and a full summary.

Events

The **Events** tab appears by default and contains a timeline for the vulnerability. Use the horizontal scroll bar or click an *event marker* to go to that event. Click event links to open them in your web browser.

The timeline can contain the following events.

Event	Description
Discovery Date	Indicates the date Tenable first observed the vulnerability.
NVD Published	Indicates the date that the National Vulnerability Database (NVD) disclosed the vulnerability.
First Tenable Coverage	Indicates the first time Tenable provided coverage for the vulnerability.
First Proof of Concept	Indicates the date Tenable first observed a proof of concept for the vulnerability.
First Functional Exploit	Indicates the date the first functional exploit for the vulnerability was released.
Consec Plugin Published	Appears when a new Container Security Scanner plugin for the vulnerability is released.
Nessus Plugin	Appears when a new Tenable Nessus plugin for the vulnerability is

Published	released.
NNM Plugin Published	Appears when a new Tenable Network Monitor plugin for the vulnerability is released.
WAS Plugin Published	Appears when a new [[[Undefined variable WebApplicationScanning.WAS]]] plugin for the vulnerability is released.
Ransomware	Indicates the first time Tenable observed ransomware events for the vulnerability.
Malware	Indicates the first time Tenable observed malware events for the vulnerability.
Emerging Threats	Indicates that Tenable is actively monitoring the vulnerability since it is being publicly discussed, has a viable proof of concept, and/or is widely used.
Exploited in the Wild	Indicates that the vulnerability has been used in a cyberattack.
Persistently Exploited	Appears each time Tenable observes that the vulnerability is being persistently exploited.
CISA Known Exploits	Indicates the date that the Cybersecurity and Infrastructure Security Agency (CISA) added the vulnerability to their Known Exploited Vulnerabilities catalog.
CISA Due-Date	Indicates the date by which federal agencies must fix vulnerabilities on the CISA Known Exploited Vulnerabilities (KEV) list.
Cyber Exposure Alert	Appears when Tenable publishes a Cyber Exposure Alert for the vulnerability.
EPSS Increased	Appears when the Exploit Prediction Scoring System (EPSS) increases (for

	example, *EPSS Increased to 65%*).
EPSS Decreased	Appears when the EPSS decreases.
EPSS Assigned	Appears when an EPSS score is assigned.
VPR Increased	Appears when the Vulnerability Priority Rating (VPR) increases (for example, *VPR Increased to 6.1*). (missing or bad snippet)
VPR Decreased	Appears when the VPR decreases. (missing or bad snippet)
VPR Assigned	Appears when a VPR score is assigned. (missing or bad snippet)

Scores

The **Scores** tab contains ring charts for VPR and EPSS along with trend charts to track how these scores have changed over time.

In addition, you can review the following **VPR Key Drivers**.

VPR Driver	Description
Age of Vulnerability	Indicates the number of days since the vulnerability was discovered.
CVSSv3 Impact Score	Indicates the NVD-provided CVSSv3 impact score from 0-10. If NVD did not provide a score, Tenable generates one.
Exploit Code Maturity	The highest level of exploit maturity for the vulnerability: **Unproven**, **PoC**, **Functional**, or **High**. Drawn from Tenable's research, as well as key external sources.

Product Coverage	Indicates the relative number of unique products affected. Values are **Low**, **Medium**, **High**, or **Very High**.
Threat Intensity	Indicates the number and frequency of recent threat events. Values are **Very Low**, **Low**, **Medium**, **High**, or **Very High**.
Threat Sources	Lists sources where relevant threat events occurred (for example, social media or the dark web). If no events were observed in the past 28 days, **No recorded events** appears.
Threat Recency	Indicates the number of days since a threat event occurred, from 0–180.

Plugins

The **Plugins** tab lists plugins that detected findings for the vulnerability.

Column	Description
Plugin ID	Indicates the ID of the Tenable plugin that detected the finding.
Name	Indicates the name of the Tenable plugin that detected the finding.
Family	Indicates the plugin family. For example, with a Tenable Nessus plugin, *Backdoors*. Or, with a Tenable One Web App Scanning plugin, *Code Execution*. To learn more, see About Plugin Families on the Tenable website.
Severity	Indicates severity for the detected vulnerability as **Low**, **Medium**, or **High**.
Type	Indicates the type of plugin: **Active**, **Compliance**, **Event**, **Passive**, or **WAS**.

Products

In the **Products** tab, view affected products by vendor. Next to a vendor, click the drop-down **>** to view a list of products.

For example, a vulnerability might have the **Vendor** *canonical* with the **Product** *linux*.

> **Tip**: Tenable curates this data. It represents all known affected products for a vulnerability, not only yours.

Summary

In the **Summary** tab, read a summary and **Copy** it to your clipboard.

How Does This Affect Me?

On the **Vulnerability Profile** page, view your affected assets and products that relate to the current vulnerability in the **How Does This Affect Me?** section. You can build queries to refine the results.

Affected Assets

The table of results in the **Affected Assets** tab has the following columns, which you can show or hide as described in Interact with a Customizable Table.

Column	Description
Asset ID	Indicates the asset's Universally Unique Identifier (UUID).
Name	The asset identifier, assigned based on the availability of specific attributes in logical order.
Operating System	The operating system for the affected asset.
IP Address	The IPv4 or IPv6 address for the affected asset.
Severity	The severity level of the vulnerabilities on the affected asset.

Sources

In the **Sources** section, search for and review contextual intelligence such as security advisories on the external websites where they appear.

This section contains a table with the following columns.

Column	Description
Source	Links to contextual intelligence about a vulnerability.
Authoritative	Indicates if the source is authoritative with a label such as *Tenable Research* or *NVD* (for the National Vulnerability Database).
Source Details	Provides more information about the source via labels added by the Tenable Research Team (for example, *Third Party Advisory*).

Vulnerability Metrics

In the right-hand **Vulnerability Metrics** pane, review key details in the following sections.

General Information

In the **General Information** section, review when a vulnerability was first discovered, how exploitable it is, and other details.

Field	Description
Tenable Discovery Date	Indicates the date Tenable first discovered the vulnerability.
NVD Published Date	Indicates the date that the National Vulnerability Database (NVD) added the vulnerability.
Exploitability	Describes how easy it is to exploit the vulnerability (for example, *Low Complexity, Network Exploitability*).

Exploit Maturity	The highest level of exploit maturity for the vulnerability: **Unproven**, **PoC**, **Functional**, or **High**. Drawn from Tenable's research, as well as key external sources.
First Proof of Concept	Indicates the date the first proof of concept for the vulnerability was released.
First Functional Exploit	Indicates the date the first functional exploit for the vulnerability was released.

Risk Profile

In the **Risk Profile** section, see if the Tenable Research Team is tracking a vulnerability, learn which categories it belongs to, and find out if it can be exploited from a remote network.

Field	Description
Categories	Indicates the categories the vulnerability belongs to, as described in Vulnerability Categories. Most vulnerabilities do not have a category.
Tenable Research Watchlist	Indicates that Tenable is actively monitoring the vulnerability since it is being publicly discussed, has a viable proof of concept, and/or is widely used.
Remotely Exploitable	Indicates if the vulnerability can be exploited from a remote network.
Proof of Concept Available	Indicates if Tenable has identified a proof of concept for this vulnerability.

Severity Metrics

In the **Severity Metrics** section, view Common Vulnerability Scoring System (CVSS) v2, v3, or v4, depending on which are available, along with their vector strings.

Field	Description
CVSSv4 Base Score	Indicates the CVSSv4 score. When not available from NVD, Tenable determines this score. To learn more, see CVSS vs. VPR.
CVSSv4 Vector	Lists a vector string with the values used to calculate the CVSSv4 score, for example: *CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H*. To learn more, see the CVSSv4 calculator on the FIRST website.
CVSSv3 Base Score	Indicates the CVSSv3 score. When not available from NVD, Tenable determines this score. To learn more, see CVSS vs. VPR.
CVSSv3 Vector	Lists a vector string with the values used to calculate the CVSSv3 score, for example: *CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H*. To learn more, see the CVSSv3 calculator on the FIRST website.
CVSSv2 Base Score	Indicates the CVSSv2 score. When not available from NVD, Tenable determines this score.
CVSSv2 Vector	Lists a vector string with the values used to calculate the CVSSv2 score.

Latest Plugin Coverage

In the **Latest Plugin Coverage** section, view the most recent Tenable Nessus and Tenable One Web App Scanning plugins to detect the vulnerability. Click the links to view plugin details on Tenable's website.

Field	Description
Nessus	Lists the release date of the newest Tenable Nessus plugin to identify the

	vulnerability.
Web App Scanning	Lists the release date of the newest [[[Undefined variable WebApplicationScanning.WAS]]] plugin to identify the vulnerability.

Identify Your Exposure

On the **Vulnerability Intelligence** page, you can review all vulnerabilities known to Tenable or only those in crucial categories such as **Recently Actively Exploited**. Then, you can compare the list of vulnerabilities to findings in your environment. This process has two parts: 1) review known vulnerabilities and, 2) compare them to your findings.

Review Known Vulnerabilities

First, build a list of known vulnerabilities to compare with your own findings.

To review vulnerabilities known to Tenable:

1. In the left navigation, click **Vulnerability Intelligence**.

   The **Vulnerability Intelligence Overview** page appears.

2. (Optional) Click a hexagon tile to choose a vulnerability category. If you want to search all vulnerabilities, click the default category to deselect it.

   In the **CVEs** tab in the lower half of the page, a table of results appears.

   > **Tip**: Under **How Does This Affect Me?** click **Findings** or **Affected Assets** to open those tabs and start reviewing your vulnerabilities.

3. (Optional) Use the *Query Builder* to refine the results, as described in Use the Query Builder.
4. (Optional) In a table row, click the dropdown **>** to view affected assets for the CVE.
5. (Optional) Click a row in the table.

   The **Vulnerability Intelligence Profile** page for the CVE appears.

Compare Known Vulnerabilities to Your Findings

Once you have built a list of known vulnerabilities, compare them with your findings in the **My Findings** tab or the **My Affected Assets** tab as follows.

Click the **My Findings** tab and do one of the following:

- Refine your results with the Query Builder.
- In a row, click the number in the **Affected Assets** column.

  The **Asset Tags** page appears. It is grouped by **Asset** and lists findings for that Tenable plugin.
- Click the dropdown **>** to display a list of assets with that finding. Then, click an **Asset Tag Name**.

  The **Asset Tag Details** page appears.

Click the **My Affected Assets** tab and do one of the following:

- Refine your results with the Query Builder.

  In a row, click the number in the **Plugin Count** column.
- The **Assets** page appears. It is grouped by **Plugin** and lists findings for that asset.
- Click the dropdown **>** to display a list of assets with that finding. Then, click an **Asset Name**.

  A list of plugins that identified findings on that asset appears.

Use the Query Builder

In the three tabs on the lower part of the **Vulnerability Intelligence** page, use the *Query Builder* to refine your search results with contextual filters.

How Queries Work

Queries are joined by *Conditions* (for example, AND). They have three components:

- **Filter** – The search criteria (for example, for a vulnerability, *Common Name*).
- **Operator** – The condition to filter on (for example, *is not equal to*).
- **Value** – The value to search (for example, a CVE ID of *CVE-2024-3272*).

Tip: You can nest queries with parentheses. For example, to search for CISA Known Exploited vulnerabilities where the VPR is greater than five or the EPSS is greater than 50, use:
Category is equal to CISA Known Exploited AND (VPR is greater than 5 OR EPSS Score is greater than 50).

Build a Query

To build a query with the Query Builder:

1. In the left navigation, click **Vulnerability Intelligence**.

   The **Vulnerability Intelligence Overview** page appears.
2. Build a list of CVEs, findings, or affected assets, as described in Identify Your Exposure.
3. Click the query box.

   The **Filters** list appears. To review the filters you can use, see Query Builder Filters.
4. In the **Filters** list, choose a filter.

   The **Operators** list appears.
5. In the **Operators** list, choose an operator.

   For a filter where the value is text or a number, the **Value Hint** box appears. Otherwise, the **Value Options** list appears.
6. Type a Value or select one from the list.
7. (Optional) Add another query (that is, type a Condition and then add a Filter, an Operator, and a Value).
8. Click **Search** or press **Enter**.

   A table of results appears.

Edit a Query

To edit a query, do one of the following.

Action	Description

Replace a query component	In the query box, click the component to replace. A list of options appears.
Delete a query component	On the query component, click the **X**.
Clear a query	On the right side of the query box, click **Clear**.

Keyboard Shortcuts

Use the following keyboard shortcuts in the Query Builder.

Shortcut	Description
Up Arrow or **Down Arrow**	Navigate lists of open-ended values such as text or numbers.
Right Arrow or **Left Arrow**	Move the cursor in your query or choose a date in the date picker.
Enter	Select a query component or date. If no component is selected, apply the query.
Esc	Close a list (for example, the **Filters** list).
Ctrl-C	Copy the highlighted text.
Ctrl-V	Paste your clipboard contents into the Query Builder.
Ctrl-Z	Undo the last action.
Ctrl-Y	Redo the last action.

Query Builder Filters

On the **Vulnerability Intelligence** page and the **Vulnerability Profile** page, use the Query Builder to refine your results. Show only the CVEs, findings, or affected assets you want to take action on.

The following table lists the filters you can use with the Query Builder and the tabs they appear in.

Filter	Description	Appears In...
ACR	Filter by Tenable-defined Asset Criticality Rating (ACR) as a number from 1 to 10.	My Findings, My Affected Assets
AES	Filter by Tenable-defined Asset Exposure Score (AES) as a number from 0 to 1000.	My Findings, My Affected Assets
Asset ID	Filter by the UUID of the asset. This value is unique to Tenable Security Center Director.	My Findings, My Affected Assets
Asset Name	Filter by asset name, for example the IPv4 address *206.206.136.40*.	My Findings, My Affected Assets
Category	Filter by category, as described in Vulnerability Categories.	CVEs, My Findings, My Affected Assets
Common Name	Filter by a vulnerability's common name, for example	CVEs, My

Filter	Description	Appears In...
	Log4Shell. Not all vulnerabilies have a common name.	Findings, My Affected Assets
CVE ID	Filter by Common Vulnerabilities and Exposures (CVE) ID, for example *CVE-2002-2024*.	CVEs
CVSSv2 Score	Filter by the CVSSv2 score for the vulnerability, for example *5.2*. When not available from NVD, Tenable determines this score. To learn more, see CVSS vs. VPR.	CVEs
CVSSv3 Attack Complexity	Filter by attack complexity, which defines how difficult it is to use a vulnerability in an attack. Choose from **High** or **Low**.	CVEs
CVSSv3 Attack Vector	Filter by attack vector, which defines an attack's location. Choose from **Adjacent**, **Network**, **Local**, or **Physical**.	CVEs
CVSSv3 Availability	Filter by the affected asset's availability. Choose from **High**, **Low**, or **None**. For example, an affected asset with *High* is completely unavailable.	CVEs
CVSSv3 Score	Filter by the CVSSv3 score for the vulnerability, for example *4.3*. When not available from NVD, Tenable determines this score. To learn more, see CVSS vs. VPR.	CVEs, My Findings, My Affected Assets
CVSSv3 Confidentiality	Filter by the expected impact of the affected asset's information confidentiality loss. Choose from **High**, **Low**, or **None**. For example, an affected asset with *High* may	CVEs

Filter	Description	Appears In...
	have a catastrophic adverse effect on your organization or customers.	
CVSSv3 Integrity	Filter by the expected impact of the affected asset's data integrity loss. Choose from **High**, **Low**, or **None**.	CVEs
CVSSv3 Privileges Required	Filter by the permission level attackers require to exploit the vulnerability. Choose from **High**, **Low**, or **None**. *None* means attackers need no permissions in your environment and can exploit the vulnerability while unauthorized.	CVEs
CVSSv3 Scope	Filter by whether a vulnerability allows attackers to compromise resources beyond an affected asset's normal authorization privileges. Choose from **Unchanged** or **Changed**. *Changed* means the vulnerability increases the affected asset's privileges.	CVEs
CVSSv3 User Interaction	Filter by whether a vulnerability requires other users (such as end users) for attackers to be able to use it. Choose from **Required** or **None**. *None* is more severe since it means that no additional user interaction is required.	CVEs
CVSSv4 Score	Filter by the CVSSv4 score for the vulnerability, for example, *4.3*. When not available from NVD, Tenable determines this score. To learn more, see CVSS vs. VPR.	CVEs, My Findings, My Affected Assets
EPSS Score	Filter by the percentage likelihood that a vulnerability will be exploited, based on the third-party Exploit Prediction	CVEs

Filter	Description	Appears In...
	Scoring System (EPSS). Type a number from 1 to 100 with up to three decimal places, for example, *50.5*.	
Exploit Maturity	Filter by exploit maturity based on sophistication and availability. This information is drawn from Tenable's own research as well as key external sources. Choose from **High**, **Functional**, **PoC**, or **Unproven**.	CVEs
First Discovered	Filter for the date a vulnerability was first identified. Use Operators to get results based on a date range, a specific date, vulnerabilities older than a date, and others.	CVEs
First Functional Exploit	Filter for the date a vulnerability was first known to be exploited. Use Operators to get results based on a date range, a specific date, vulnerabilities older than a date, and others.	CVEs
First Proof of Concept	Filter for the date a vulnerability's first proof of concept was found. Use Operators to get results based on a date range, a specific date, vulnerabilities older than a date, and others.	CVEs
IP Address	Filter for affected asset IPv4 and IPv6 addresses as a single IP, an IP range, or an IP Classless Inter-Domain Routing (CIDR) block. For example, type *172.16.2.1-172.16.2.100, ::ffff:c0a8:102*.	My Findings, My Affected Assets
Last Seen	Filter for the date a finding affected or asset last appeared on a scan. Use Operators to get results based on a date range, a specific date, vulnerabilities older than a date,	My Findings, My Affected

Filter	Description	Appears In...
	and others.	Assets
Operating System	Filter by assets running the specified operating system.	My Findings, My Affected Assets
Plugins Available	Filter by whether or not a vulnerability currently has a Tenable plugin that detects it. Choose from **Yes** or **No**.	CVEs
Plugin Family	Filter by the family of the Tenable plugin that detected the vulnerability. For example, *Service detection*.	My Findings, My Affected Assets, Plugins
Plugin ID	Filter by the ID of the Tenable plugin that detected the vulnerability, for example *157288*. To look up plugin IDs, go to the Tenable website.	CVEs, My Findings, My Affected Assets, Plugins
Plugin Name	Filter by the name of the Tenable plugin that detected the vulnerability, for example *TLS Version 1.1 Protocol Deprecated*.	My Findings, My Affected Assets, Plugins
Plugin Type	Filter by the type of Tenable plugin that detected the vulnerability. For example, *remote*.	My

Filter	Description	Appears In...
		Findings, My Affected Assets, Plugins
Repository	Filter for assets with associated vulnerability data in the specified repository.	My Findings, My Affected Assets
Severity	Filters by the vulnerability's CVSS-based severity. To learn more, see CVSS vs. VPR.	My Findings, My Affected Assets, Plugins
VPR	Filter by the Tenable-calculated Vulnerability Priority Rating (VPR) score, as a number from 1 to 10. (missing or bad snippet) **Note**: A finding's VPR is based on the VPR of the plugin that identified it. When plugins are associated with multiple vulnerabilities, the highest VPR appears.	CVEs, My Findings, My Affected Assets
VPR Threat Intensity	Filter for a vulnerability's Tenable-calculated threat intensity based on the number and frequency of threat events. Choose from **Very Low**, **Low**, **Medium**, **High**, or **Very High**.	CVEs

CVEs

On the **Vulnerability Intelligence Overview page**, the **CVEs** tab shows vulnerabilities from Tenable's database. All vulnerabilities appear by default, but you can refine the results with vulnerability categories and the query builder.

The table in the **CVEs** tab has the following columns, which you can show or hide as described in Interact with a Customizable Table.

Column	Description
CVE ID	Indicates the Common Vulnerability and Exposure (CVE) identifier for the vulnerability, as assigned by the CISA-sponsored CVE Program.
Name	Indicates the informal name of the vulnerability (for example, *Log4Shell*). Not all vulnerabilities have a common name.
VPR	The Tenable-calculated Vulnerability Priority Rating (VPR) score from 0.1 to 10.
VPR (Beta)	The Tenable-calculated Vulnerability Priority Rating (VPR) score from 0.1 to 10. For more information, see Enhancements to Tenable's VPR.
CVSS v2	Indicates the CVSS v2 score for the vulnerability. When not available from NVD, Tenable determines this score. To learn more, see CVSS vs. VPR.
CVSS v3	Indicates the CVSS v3 score for the vulnerability. When not available from NVD, Tenable determines this score. To learn more, see CVSS vs. VPR.
CVSS v4	Indicates the CVSS v4 score for the vulnerability. When not available from NVD, Tenable determines this score. To learn more, see CVSS vs. VPR.
EPSS	Indicates the likelihood that the vulnerability will be actively exploited, based on the third-party Exploit Prediction Scoring System (EPSS).
Exploit Maturity	The highest level of exploit maturity for the vulnerability: **Unproven**, **PoC**, **Functional**, or **High**. Drawn from Tenable's research, as well as key external

	sources.
First Discovered	Indicates the date the vulnerability was first identified.
First Exploited	Indicates the date of the vulnerability's first-known exploitation.
POC	Indicates the date the vulnerability's first proof of concept was discovered.
Plugins	Lists the IDs for the Tenable plugins that detected the vulnerability.

My Findings

On the **Vulnerability Intelligence Overview** page, the **My Findings** tab shows all active, new, or resurfaced findings in your environment that are being tracked by Tenable One Vulnerability Management. Refine the results with vulnerability categories and the query builder.

The **My Findings** tab has the following columns, which you can show or hide as described in Interact with a Customizable Table.

Column	Description
VPR	The Tenable-calculated Vulnerability Priority Rating (VPR) score from 0.1 to 10. **Note**: A finding's VPR is based on the VPR of the plugin that identified it. When plugins are associated with multiple vulnerabilities, the highest VPR appears.
VPR (Beta)	The Tenable-calculated Vulnerability Priority Rating (VPR) score from 0.1 to 10. For more information, see Enhancements to Tenable's VPR. **Note**: A finding's VPR is based on the VPR of the plugin that identified it. When plugins are associated with multiple vulnerabilities, the highest VPR appears.
Plugin Name	Indicates the name of the Tenable plugin that detected the finding.

Plugin ID	Indicates the ID of the Tenable plugin that detected the finding.
Affected Assets	Indicates the number of affected assets. Click the number to open the **Asset Tag Details** page.
CVES	The CVE IDs associated with the finding.
CVSSv2	Indicates the Common Vulnerability Scoring System (CVSS) v2 score for the finding.
CVSSv3	Indicates the CVSS v3 score for the finding.
CVSSv4	Indicates the CVSS v4 score for the finding.

Affected Assets

In any findings row, click the dropdown **>** to reveal a table of assets on which that finding appears, with the following columns.

Column	Description
Asset Name	The asset identifier, assigned based on the availability of specific attributes in logical order.
Operating System	Indicates the operating system the asset is running.
IP Address	Indicates the IPv4 or IPv6 address for the asset.
Repository	Indicates the repository associated with the asset.
Plugin Count	Indicates the number of plugins that discovered findings on the asset.
ACR	TheAsset Criticality Rating for the asset.
AES	The Asset Exposure Score for the affected asset.

Last Seen	Indicates the date when the asset last appeared on a scan.

My Affected Assets

On the **Vulnerability Intelligence Overview** page, the **My Affected Assets** tab shows all assets in your environment with a finding that has not yet been fixed. Refine the results with vulnerability categories and the query builder.

The **My Affected Assets** tab has the following columns, which you can show or hide as described in Interact with a Customizable Table.

Column	Description
Name	The asset identifier, assigned based on the availability of specific attributes in logical order.
Operating System	Indicates the operating system the asset is running.
IP Address	Indicates the IPv4 or IPv6 address for the asset.
Repository	Indicates the repository associated with the asset.
Plugin Count	Indicates the number of Tenable plugins that identified findings on the asset. Click the number to review details on the **Assets** page.
ACR	(Tenable Security Center+ only) TheAsset Criticality Rating for the asset. **Note:** If you upgrade to Tenable Security Center+, this column will not display data until an import runs and the findings are refreshed.
AES	(Tenable Security Center+ only) The Asset Exposure Score for the affected asset.

	Note: If you upgrade to Tenable Security Center+, this column will not display data until an import runs and the findings are refreshed.
CVES	The CVE IDs associated with the asset.

Plugins

In any asset row, click the dropdown **>** to reveal a table of plugin results for the findings on that asset, with the following columns.

Column	Description
VPR	The Tenable-calculated Vulnerability Priority Rating (VPR) score from 0.1 to 10. **Note**: A finding's VPR is based on the VPR of the plugin that identified it. When plugins are associated with multiple vulnerabilities, the highest VPR appears. (missing or bad snippet)
Severity	Indicates the vulnerability's severity based on the Common Vulnerability Scoring System (CVSS).
Plugin Name	Indicates the name of the Tenable plugin that detected the finding.
Plugin ID	Indicates the ID of the Tenable plugin that detected the finding.
Findings	Indicates the number of findings detected on the asset.
CVSSv2	Indicates the CVSSv2 score for the finding.
CVSSv3	Indicates the CVSSv3 score for the finding.
CVSSv4	Indicates the CVSSv4 score for the finding.

Vulnerability Categories

The **Vulnerability Intelligence** page breaks down key vulnerabilities from Tenable's database into curated categories that you select from hexagon-shaped tiles.

While most vulnerabilities do not belong to categories, the ones that do require quick action when found in your environment! To learn how to compare your findings to one of these categories, see Identify Your Exposure.

You can choose from the following categories.

Category	Description
Emerging Threats	Vulnerabilities being actively monitored by Tenable in three areas: • **Vulnerabilities Being Monitored** – Publicly discussed, but no exploit or proof of concept has been disclosed. • **Vulnerabilities of Interest** – Publicly discussed and have a proof of concept that could lead to widespread use by attackers. • **Vulnerabilities of Concern** – Widely discussed and large-scale abuse by attackers is being observed.
CISA Known Exploited	Vulnerabilities that appear in the CISA Known Exploited Vulnerabilities Catalog. CISA suggests that you prioritize remediation efforts for these vulnerabilities since they are known to cause immediate harm.
In the News	Vulnerabilities being widely reported in the press with notable coverage over the past 30 days.
Recently Actively Exploited	Vulnerabilities with notable coverage in the press over the past 30 days, and for which Tenable has evidence of active exploitation.
Ransomware	Vulnerabilities used in current or historical ransomware attacks, as determined from evidence gathered by the Tenable Research team.

Persistently Exploited	Vulnerabilities being leveraged by threat actors over an extended period of time in targeted attacks, ransomware, or malware campaigns. These vulnerabilities are manually curated by the Tenable Research team.
Top 50 VPR	The top 50 vulnerabilities by Vulnerability Priority Rating (VPR).

Reports

You can create reports in Tenable Security Center Director to share data with users in other organizations. For more information about which users can access what data, see Tenable Security Center Architecture.

Tenable provides reporting through an assortment of report templates and customizable report formats, including PDF and CSV.

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.

In Tenable Security Center Director, organizational users can create custom reports or template-based reports, as described in Create a Custom Report or Create a Template Report.

Note: To create custom PDF reports and template-based reports, you must install either the Oracle Java JRE or OpenJDK (along with their accompanying dependencies) on the system hosting the Tenable Security Center.

Tip: Tenable provides report templates through the Tenable Security Center feed. For a complete index of Tenable-provided report templates, see the Tenable Security Center Report Templates blog.

For more information, see:

- Manage Reports
- Manage Report Results

- CyberScope and DISA Report Attributes
- Report Images

Manage Reports

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

On the **Reports** page of Tenable Security Center, you can manage report definitions and launch reports. For more information, see Reports.

Create a Custom Report

For more information, see Reports.

Before you begin:

- If you want to create a CyberScope, DISA ASR, DISA ARF, or DISA Consolidated ARF report, confirm an administrator user enabled the corresponding 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 Security Center Director via the user interface.
2. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.
3. At the top of the table, click **Add**.

   The **Report Template** page appears.
4. In the **Other** section, click a report tile. For more information, see Report Templates.
5. Configure the options for the report.

Tenable Security Center displays options relevant to the report format you selected.

6. (Optional) Edit the report outline.
7. Click **Submit** to save your report.

   Tenable Security Center Director saves your configuration.

Create a Template Report

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 Security Center Director via the user interface.
2. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.
3. At the top of the table, click **Add**.

   The **Report Template** page appears.
4. Do one of the following to locate a specific template:
   - 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.

   - In the **Common** section, click a template category to view the related templates. For more information, see Report Templates.
5. Click a template report.

   > **Note:** Each template description specifies which Tenable Security Center data must be available to obtain a complete report. For more information, see Data Required for Template-Based Reports.

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 Security Center 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 more information, see Report Options.

    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) Customize the report outline, as described in Edit a Report Outline.

For example, you might want to use text elements to add your business context to template-based chapters.

Launch a Report on Demand

To launch a report on demand:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.
2. (Optional) Filter the reports table, as described in Apply a Filter.
3. In the table, right-click the row for the report you want to launch.

   -or-

   Select the check box for the report you want to launch.

   The actions menu appears.
4. Click **Launch**.
5. (Optional) Monitor the status of the report in the **Report Results** page.

   To view this page, do one of the following:

   - In the launch notification message, click **View Report Results**.
   - In the left navigation, click **Reporting > Report Results**.

   > **Note:** In the **Report Results** page, you can also stop the currently running report.

Stop a Running Report

If you want to stop a report that is currently running:

1. Click **Reporting** > **Report Results**.

   The **Report Results** page appears.
2. (Optional) Filter the report results table, as described in Apply a Filter.
3. Right-click the row for the report you want to stop, and click **Stop**.

Tenable Security Center stops the report run.

> **Note:** You cannot restart a stopped report run. You can only launch the report again.

Report Templates

Tenable Security Center provides a selection of report templates and customizable report formats. You can configure a Tenable-provided report template or you can create a fully customized report from one of the available formats. For more information, see Reports.

For a complete index of Tenable-provided report templates, see the Tenable Security Center Report Templates blog.

Template	Description
Common	
Compliance & Configuration Assessment	Reports that aid with configuration, change, and compliance management.
Discovery & Detection	Reports that aid in trust identification, rogue detection, and new device discovery.
Executive	Reports that provide operational insight and metrics geared towards executives.
Monitoring	Reports that provide intrusion monitoring, alerting, and analysis.
Security Industry Trends	Reports related to trends, reports, and analysis from industry leaders.
Threat Detection & Vulnerability	Reports that aid with identifying vulnerabilities and potential threats.

Assessments	
Other	
PDF	Create a Portable Document Format (PDF) report that can be viewed universally.
CSV	Create a Comma Separated Values (CSV) report that can be imported into spreadsheets or databases.
DISA ARF	(Requires Report Generation configuration) Create a report that meets the standards of the Defense Information Systems Agency Assessment Results Format (DISA ARF).
DISA Consolidated ARF	(Requires Report Generation configuration) Create a report that meets the standards of the Defense Information Systems Agency Consolidated Assessment Results Format (DISA Consolidated ARF).
DISA ASR	(Requires Report Generation configuration) Create a report that meets the standards of the Defense Information Systems Agency Assessment Summary Results (DISA ASR).
CyberScope	(Requires Report Generation configuration) Create a report that meets CyberScope reporting standards to support FISMA compliance.

Data Required for Template-Based Reports

Each report template description contains icons that represent which types of data must be available on Tenable Security Center to obtain a complete report.

Hover the cursor over the icon to display the label.

Icon	Label	Action Required

	Asset Required	Configure an asset repository and store scan results in the repository; see Local Repositories and Asset Repositories.
	Audit File Required Compliance Data Required	Upload audit files and add them to your scan policy; see Audit Files and Scan Policies.
	Local Checks Required	Configure and run credentialed scans; see Active Scans.
	Mobile Data Required	Configure a mobile repository and store scan results in the repository; see Mobile Repositories.
NS	Active Data Required	Configure a Tenable Nessus scanner and run active scans. For more information, see Tenable Nessus Scanners and Active Scans.
PVS	Passive Data Required	Configure a Tenable Network Monitor (NNM) scanner; see Tenable Network Monitor (PVS).

Report Options

In Tenable Security Center, you can configure the options described below for both custom and template reports. For information on how to create reports, see Create a Custom Report and Create a Template Report.

The option descriptions on this page are grouped as they appear on the **Add Report** and **Edit Report** pages. In the options tables, the **Relevant Reports** column specifies which report types use each option.

> **Note:** Tenable Security Center 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 Security Center 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

Option	Description	Relevant Reports
Name	Name assigned to the report.	Any
Description	Descriptive text for the report.	Any
Schedule	Determines how often the report runs. Options are **On Demand**, **Now**, **Once**, **Daily**, **Weekly**, or **Monthly**. When you select a frequency from the drop-down box, Tenable Security Center displays additional options for the selected time frame.	Any
Attribute Sets	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. For more information, see CyberScope and DISA Report Attributes.	DISA ARF, DISA Consolidated ARF, CyberScope
ASR Content	When creating a report, this drop-down box offers a	DISA ASR,

Option	Description	Relevant Reports
	selection of Benchmark, IAVM, CVE, or Plugin ID to be included.	DISA Consolidated ARF
ASR Record Format	This drop-down box determines the format (Summary or Detail) of the DISA ASR report.	DISA ASR
Include ARF	When enabled, allows for the inclusion of a DISA attribute set for the report.	DISA ASR
Benchmarks	Benchmarks are generated after a scan using certain audit files that have been successfully run against at least one target system.	DISA ASR, DISA Consolidated ARF, CyberScope

Report Options

Option	Description	Relevant Reports
Style	A compound value that specifies the report style, paper size, and orientation. For example, **Plain, Letter** 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	PDF

Option	Description	Relevant Reports
	footer logo on the cover page **Note:** If an administrator configured a Classification Type banner, plain report styles are the only options listed. Paper sizes include: • **Letter** – the standard 8.5 inches x 11 inches letter 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. • **A4** – the standard 8.27 inches x 11.69 inches A4 size Orientation options include: • **Portrait** – vertical **Note:** Portrait is the default orientation, used by options that do not explicitly state an orientation. For example, the orientation for **Plain, Letter** is vertical. • **Landscape** – horizontal	
Include Cover Page	Include a cover page in the report. Cover pages include: • a cover logo • the scan **Name** • the date and time you generated the report • the date and time Tenable Security Center imported the scan results, if you generated the report from scan results	PDF

Option	Description	Relevant Reports
	• 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 Contents	Include a table of contents with the report.	PDF
Include Index	Include an Index with the report.	PDF
Cover Logo	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 Report Images. **Note:** The Plain report style suppresses this footer logo on the cover page.	PDF
Footer Logo	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 Report Images.	PDF
Watermark	Specifies a watermark for each page of the report. The default is no watermark. To add a custom watermark, see Report Images.	PDF
Encrypt PDF	Protect the PDF with a password and 256-bit Advanced Encryption Standard (AES) encryption. When enabled, the	PDF

Option	Description	Relevant Reports
	Password text box appears. Enter a password to use to open the report and view its contents.	

Definition Options

Tenable Security Center displays definition options relevant to the report or report element type.

Option	Description	Relevant Reports
Add Chapter	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 Add a Custom Chapter to a Report and Edit a Report Outline.	PDF
Add Template Chapter	A predefined chapter from a Tenable-provided report template. For more information, see Add a Template Chapter to a Report.	PDF
Query	A list of predefined queries you can use to retrieve data for the report. For more information, see Queries.	CSV, DISA ARF, DISA Consolidated ARF, DISA ASR, CyberScope; Iterator, Table, and Chart elements in PDF
Type	The type of data to include in the report.	CSV; Iterator, Table, and Chart elements in PDF

Option	Description	Relevant Reports
Source	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: • If **Type** is set to **Vulnerability**, valid **Source** values are: ◦ **Cumulative**–All vulnerabilities, regardless of whether the vulnerabilities have been remediated or not ◦ **MItigated**–Remediated vulnerabilities ◦ **Individual Scan**–Vulnerabilities identified in a specific scan **Note:** If you select **Individual Scan**, Tenable Security Center displays the **Selected Scan** option, which allows you to select a scan to use as the basis of the report: a. Click one of the predefined date ranges, or click **Custom Range** and enter starting and ending days for the range. b. Click **Fetch Scans** to view a list of possible scans within the date range. c. Click the scan you want to use in the drop-down box. • If **Type** is set to **Mobile**, Ticket, or Alert, this option is absent.	CSV, DISA ARF, DISA Consolidated ARF, DISA ASR, CyberScope; Iterator, Table, and Chart elements in PDF

Option	Description	Relevant Reports
	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.	
Tool	Select the tool Tenable Security Center uses to analyze the data in the report.	CSV; Iterator, Table, and Chart elements in PDF
Filters	Specifies additional criteria to refine report data. For more information, see Manage Filter Components for a Non-Chapter Report.	CSV, DISA ARF, DISA Consolidated ARF, DISA ASR, CyberScope; Iterator, Table, and Chart elements in PDF
Find/Update Filters	This option appears after you add at least one chapter to the report. For more information, see Manage Filter Components for Multiple Elements in a Chapter Report.	PDF

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.

Option	Description	Relevant Reports
Results Displayed	The number of results included in the CSV file.	CSV; Iterator, Table, Bar Chart, and Pie Chart elements in PDF
Sort Column	The column that Tenable Security Center 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
Sort Direction	The sort direction for results in the CSV file.	CSV; Iterator, Table, Bar Chart, and Pie Chart elements in PDF
Display Columns	The columns included in the results file. Available columns depend on **Definition** options you select. **Tip:** The **Display Columns** appear in the results file in the order in which you select them.	CSV; Iterator, Table, Bar Chart, and Pie Chart elements in PDF

Distribution Options

Distribution options specify the actions Tenable Security Center takes when a report run completes.

Option	Description	Relevant Reports
Email Users	Select Tenable Security Center users to whom Tenable Security Center emails the completed report. The drop-down list includes only users with defined email addresses.	Any
Email Addresses (cc)	Add CC email addresses where Tenable Security Center emails the completed report. You can specify multiple email addresses, separated by commas.	Any
Email Addresses (bcc)	Add Bcc email addresses where Tenable Security Center emails the completed report. You can specify multiple email addresses, separated by commas.	Any
Share	Allows you to select which Tenable Security Center users within your organization can view the completed report in Tenable Security Center. Use this option if organizational policies prohibit emailing potentially sensitive data.	Any
Publishing Sites	Allows you to select predefined publishing sites where Tenable Security Center uploads the completed report. For more information, see Publishing Sites Settings.	Any

Manage Report Definitions

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

View a Report Definition

To view a report definition:

1. In the left navigation, 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. In the table, right-click the row for the report definition you want to view.

   The actions menu appears.
4. Click **View**.

   Tenable Security Center 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

You can share a copy of a report definition with other users in your organization in Tenable Security Center. 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. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.
2. In the table, right-click the row for the report definition you want to copy.

   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 Security Center copies the report definition to the other accounts you specified. The copy appears, named **Copy of *DefinitionName***.

Edit a Report Definition

In Tenable Security Center, you can edit both custom reports and reports based on templates.

To edit a report definition:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.
2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.
3. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.
4. Modify the report options.

   > **Note:** Tenable Security Center displays options relevant to the report type.

5. (PDF and template reports only) Edit the report outline.
6. Click **Submit** to save your changes to the report.

Import a Report Definition

In Tenable Security Center, you can only import XML files in the same format used to export report definitions. This feature is useful for organizations running multiple Tenable Security Center

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. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.
3. At the top of the table, click **Import Report**.
4. In the **Name** box, type a name for the report.
5. Click **Choose File** next to the **Report Definition** box.
6. Browse to the local copy of the report definition XML file.
7. Click **Import**.

   Tenable Security Center imports the report definition.
8. (Optional) Edit the report definition as desired.

Export a Report Definition

In Tenable Security Center, you can export a report definition as an `.xml` file. This feature is useful for organizations running multiple Tenable Security Center deployments to provide consistent reports without duplicating the work needed to create definition templates.

To export a report definition:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.
2. In the table, right-click the row for the report definition you want to export.

   The actions menu appears.
3. Click **Export**.

4. Click the export option you want to use:

Option	Description
Keep All References	Export the report definition with object references intact. Users who meet the following requirements can use an imported report definition with intact object references: • The user must be in the same organization as the user who exported the report definition. • The user must have access to all relevant objects in the report definition.
Remove All References	Export the report definition with object references removed, altering the definitions of the components. Any user can use an imported report definition with object references removed.
Replace With Placeholders	Export the report definition with object references replaced with their respective names. Users must replace the placeholder names with applicable objects available to their organization in order to use an imported report definition with placeholder names.

Tenable Security Center downloads the report definition to your computer.

Delete a Report Definition

To delete a report definition:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. To delete a single report definition:

   a. In the table, right-click the row for the report definition you want to delete.

      The actions menu appears.

   To delete multiple report definitions:

   a. In the table, select the check box for each report definition you want to delete.

      The available actions appear at the top of the table.

3. Click **Delete**.
4. Click **Delete** to confirm the deletion.

   Tenable Security Center deletes the report definition.

   > **Note:** Tenable Security Center retains any report results associated with the deleted definition. You must manually delete results associated with the report.

Manage Report Outlines

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

In Tenable Security Center, the report outline allows you to modify the structure of a PDF or template-based report.

The outline consists of the following components:

Component	Outline Level	Description
chapter	primary	Highest-level component. Can contain any type of element (grouping, text, chart).
element	subordinate	A grouping, text, or chart element. Can be nested in a chapter or grouping component.

Edit a Report Outline

To edit a report outline:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, 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** at the top of the outline.
   - 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 Security Center 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

In Tenable Security Center, you can add custom chapters to PDF or template-based reports.

To add a custom chapter to a report definition:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, click **Definition**.

   The report outline appears. This outline is, by default, expanded. For more information, see Edit a Report Outline.

4. At the bottom 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 Security Center 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

In Tenable Security Center, you can add template chapters to template reports and custom PDF reports.

To add a template-based chapter to a report definition:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, click **Definition**.

   The report outline appears. This outline is, by default, expanded. For more information, see Edit a Report Outline.

4. At the bottom 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 Security Center 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

You can add or edit elements within chapters or grouping elements in Tenable Security Center reports.

To add or edit a report element:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, 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

Grouping elements in Tenable Security Centerreports include:

Type	Description	Relevant Reports
Group	Groups associated elements on the same page.	PDF
Section	Allows you to organize content within chapters.	PDF
Iterator	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.	PDF

To configure a grouping element:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, 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:

Option	Action
Name	Type a name for the element.
Location	Select a location for the element in the report.
Style	Select a style for the element.

    - Add a section to the report.
        a. In the **Grouping** section, click the **Section** icon.
        b. Configure the following options:

Option	Action
Name	Type a name for the element.
Location	Select a location for the element in the report.
Style	Select a style for the element.

    - Add an iterator to the report.
        a. In the **Grouping** section, click the **Iterator** icon.
        b. Configure the following options:

Option	Action

General	
Name	Type a name for the element.
Location	Select a location for the element in the report.
Style	Select a style for the element.
Definition	
Query	Select a predefined query to define the data included in the element. For more information, see Queries.
Type	Select the type of data to include in the element. Iterator elements support vulnerability or event data only.
Source	Select the source of the data included in the element. Valid values for this field differ based on the setting of the **Type** option: • If **Type** is set to **Vulnerability**, valid **Source** values are: ◦ **Cumulative**–All vulnerabilities, regardless of whether the vulnerabilities have been remediated or not ◦ **MItigated**–Remediated vulnerabilities ◦ **Individual Scan**–Vulnerabilities identified in a specific scan **Note:** If you select **Individual Scan**, Tenable Security Center displays the **Selected Scan** option, which allows you to select a scan to use as the basis of the report:

	a. Click one of the predefined date ranges, or click **Custom Range** and enter starting and ending days for the range. b. Click **Fetch Scans** to view a list of possible scans within the date range. c. Click the scan you want to use in the drop-down box.
Filters	Specify additional criteria to refine element data. See Manage Report Filters
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 Security Center uses to sort the iteration data.
Sort Direction	Select the sort direction for the iteration data.
Header	Select the columns you want to include in the iteration data.

Information	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

Text elements in Tenable Security Center reports include:

Type	Description	Relevant Reports
Matrix	Data in a chart layout.	PDF
Table	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 Security Center presents the user with the ability to choose a vulnerability-centric report (a listing of vulnerabilities with all associated hosts).	PDF
Paragraph	Descriptive text that can be inserted anywhere in the report. Use this option to describe table elements or report output for the viewer.	PDF
Assurance Report Card	An element based on the results of a selected Assurance Report Card.	PDF

To configure a text element in a report:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, 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:

Option	Action
Name	Type a name for the element.
Location	Select a location for the element in the report.
Style	Select a style for the element.
Text	Type the text of the paragraph.

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:

Option	Action
Name	Type a name for the element.
Location	Select a location for the element in the report.
Style	Select a style for the element.
Assurance Report Card	Select the Assurance Report Card (ARC) you want to add to the report. For more information on ARCs, see Assurance Report Cards.

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

A matrix element is a type of text element you can insert into a Tenable Security Center 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. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, 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:

Option	Action
Name	Type a name for the element.

Location	Select a location for the element in the report.
Style	Select a style for the element.

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 Security Center 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 in a Chapter Report.
     f. In the **Rules** section, click **Add Rule** to add a rule.

        -or-

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 Security Center inserts the copied column to the right of the original column

  For rows, Tenable Security Center 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

Current Vulnerabilities

	New IP's	Info	Low	Medium	High	Critical
< 7 Days	895	895	62	67	24	21
8 - 14 Days	43	43	7	20	11	9
15 - 21 Days	5	5	12	21	13	4
22 - 30 Days	1	1	2	2	2	2

Configure a Table Element in a Report

A table element is a type of text element you can insert into a Tenable Security Center 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. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, 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:

Option	Action
Name	Type a name for the element.

Location	Select a location for the element in the report.
Style	Select a style for the element.

6. Configure the **Data** options:

Option	Description
Type	Equivalent to the **Definition** option of the same name in Report Options.
Query	
Source	
Tool	
Filters	

7. Configure the **Display** options:

Option	Description
Results Displayed	Equivalent to the **Display** option of the same name in Report Options.
Sort Column	
Sort Direction	
Display Columns	

8. Click **Submit** to save your changes to the element.
9. Click **Submit** to save your changes to the report.

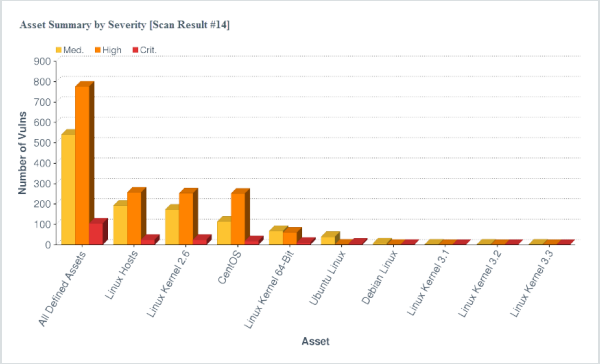
Example

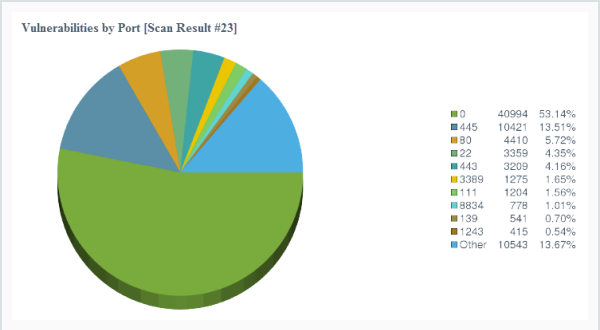
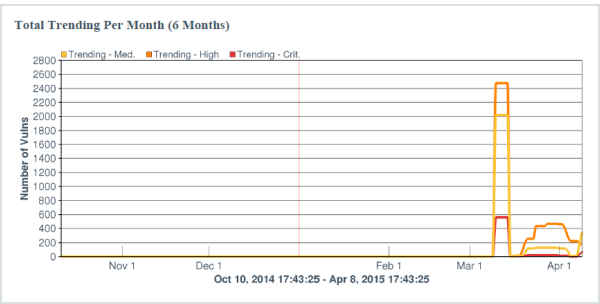
Highest Ranked Asset Vulnerability Index [Scan Result #23]

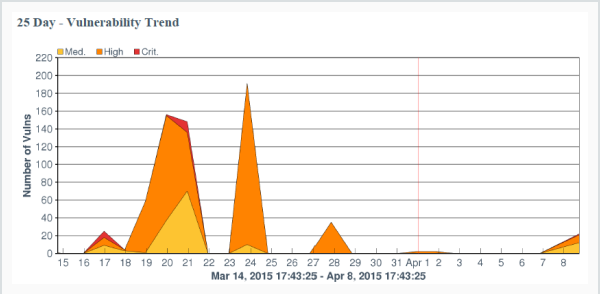
Asset	Score	Total	Med.	High	Crit.
All Defined Assets	13593	1423	541	777	105
Linux Hosts	4189	476	193	257	26
Linux Kernel 2.6	4092	453	174	253	26
CentOS	3625	386	115	252	19
Linux Kernel 64-Bit	1294	141	68	61	12
Ubuntu Linux	380	48	40	2	6
Debian Linux	74	10	8	1	1
Linux Kernel 3.1	9	3	3	0	0
Linux Kernel 3.2	6	2	2	0	0
Linux Kernel 3.3	6	2	2	0	0

Configure a Charts Element in a Report

Charts elements in Tenable Security Center reports include:

Option	Description	Relevant Reports
Bar Chart	Click to add a bar chart element to the report. 	PDF
Pie Chart	Click to add a pie chart element to the report.	PDF

Option	Description	Relevant Reports
		
Line Chart	Click to add a line chart element to the report.  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.	PDF
Area Chart	Click to add an area chart element to the report.	PDF

Option	Description	Relevant Reports
	 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. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, 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:

Option	Action
Name	Type a name for the element.
Location	Select a location for the element in the report.
Style	Select a style for the element.

6. For bar charts and pie charts, configure the following **Data** options:

Option	Action
Type	Equivalent to the option the **Definition** option of the same name in Report Options.
Query	
Source	
Tool	
Filters	

7. For line charts and area charts, configure the following **Data** options:

Option	Action
Data Type	Valid values are **Relative** and **Absolute**. Use to configure the x-axis of the chart.
Data Range	Use to configure the x-axis of the chart: • If you select **Relative** for **Data Type**, select a relative date range. • If you select **Absolute** for **Data Type**, select a specific start and end date for the data.
Series	Use to configure the y-axis of the chart. Line charts and area charts require that you configure at least one series.

8. For bar charts and pie charts, configure the following **Display** options:

Option	Action
Results Displayed	Equivalent to the **Display** option of the same name in Report Options.
Sort Column	
Sort Direction	
Display Columns	

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

In Tenable Security Center, you can reorder chapters and elements in a PDF, CSV, or template-based report.

To reorder report chapters and elements:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, 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** drop-down box.

5. Click **Submit** to save your changes to the report.

Manage Report Filters

Required Tenable Security Center 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).

In Tenable Security Center, PDF and template-based reports use a chapter structure, so you can specify different filters for individual chapter elements of those reports. 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.

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 in a Chapter Report
- Manage Filter Components for Multiple Elements in a Chapter Report
- Manage Filter Components for a Non-Chapter Report

Manage Filter Components for a Single Element in a Chapter Report

To manage filter components for a single element in a chapter report in Tenable Security Center:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, 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 Security Center prompts you to type the value you want to filter for or to select from valid values and operators.

> **Note:** If Tenable Security Center 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 pencil 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 Security Center 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 in a Chapter Report

When managing filter components for a chapter report in Tenable Security Center, 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.

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. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.
2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.
3. On the left side of the page, click **Definition**.

   The report outline appears. This outline is, by default, expanded. For more information, see Edit a Report Outline.
4. At the top 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 Security Center 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 in a Chapter Report.

2. Click **Update Filters**.

   Tenable Security Center 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

In Tenable Security Center, 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.

To manage filter components for a non-chapter report:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.
2. In the reports table, click the name of the report you want to edit.

-or-

Right-click the row for the report you want to edit, and click **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 Security Center 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 Security Center 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.

Manage Report Results

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

On the **Report Results** page of Tenable Security Center, 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. For more information, see Reports.

View a Report Result

To view a successful report result:

1. Click **Reporting** > **Report Results**.

   The **Report Results** page appears.
2. (Optional) Filter the report results table, as described in Apply a Filter.
3. Right-click the row for the report result you want to view.

   The actions menu appears.
4. Click **View**.

   The report appears.
5. (Optional) To download the report result to your computer, click **Download**.

   The report result downloads.
6. (Optional) To delete the report result, click **Delete**.

   Tenable Security Center deletes the report result.

Download a Report Result

To download a successful report result to your computer:

1. Click **Reporting** > **Report Results**.

   The **Report Results** page appears.
2. (Optional) Filter the report results table, as described in Apply a Filter.
3. Do one of the following:
   - In the Results table, click the name of the report.
   - Right-click the row for the report result.

     The actions menu appears.

     a. Click **Export**.
   - Select the check box for the report result.

     At the top of the table, click **Download**.

Publish a Report Result

To publish a successful report result:

1. Click **Reporting** > **Report Results**.

   The **Report Results** page appears.
2. Right-click the row for the report result you want to publish.

   The actions menu appears.
3. Click **Publish**.

   The **Publish Report Results** window appears.
4. Search for and select a publishing site.
5. Click **Publish**.

   Tenable Security Center publishes the report result.

Email a Report Result

To email a copy of a successful report result to specific users:

1. Click **Reporting** > **Report Results**.

   The **Report Results** page appears.
2. (Optional) Filter the report results table, as described in Apply a Filter.
3. Right-click the row for the report result you want to email.

   The actions menu appears.
4. Click **Email**.
5. Do one of the following:
   - Use the **Group** and **User** boxes to select the Tenable Security Center user or users you want to receive the report result.
   - Type the email address of recipients who are not Tenable Security Center users.
6. Click **Submit**.

   Tenable Security Center sends the report result.

Copy a Report Result

> **Note:** To share report results, you and the recipient must belong to the same group. Alternatively, your user role must have the **Share Objects Between Groups** permission enabled.
> For more information, see Organizations and Groups and User Roles.

To share a copy of a successful report result with other Tenable Security Center user accounts:

1. Click **Reporting** > **Report Results**.

   The **Report Results** page appears.
2. (Optional) Filter the report results table, as described in Apply a Filter.
3. Right-click the row for the report result you want to copy.

   The actions menu appears.
4. Click **Copy**.
5. In the **Group** box, select the group you want to grant access to a copy of the report result.

6. Specify a user or users that you want to grant access to a copy of the report result.
7. Click **Copy**.

   Tenable Security Center copies the report result to the other accounts you specified. The copy appears, named **Copy of *ResultName***.

View Errors for a Failed Report

To view error conditions for a failed report:

1. Click **Reporting** > **Report Results**.

   The **Report Results** page appears.
2. (Optional) Filter the report results table, as described in Apply a Filter.
3. Click the name of the failed result in the results table.

   The **View Report Results** page appears.
4. Review the **Error Details** section.

For more information about errors in Tenable Security Center Director, see Error Messages.

Delete a Report Result

To delete a report result:

1. Click **Reporting** > **Report Results**.

   The **Report Results** page appears.
2. (Optional) Filter the report results table, as described in Apply a Filter.
3. Right-click the row for the report result you want to delete.

   The actions menu appears.
4. Click **Delete**.

   A confirmation window appears.
5. Click **Delete** to confirm the deletion.

   Tenable Security Center deletes the report result.

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.

General Option	Description
Name	A name for the attribute.
Description	(Optional) A description for the attribute.
Type	The type of attribute you want to create. Your **Type** selection determines the other options you must configure: CyberScope Options or DISA Options.

CyberScope Options

The following table describes the additional options to configure when configuring a **CyberScope** attribute.

Option	Description
Reporting Component	The CyberScope value for a reporting component (e.g., **Department of Justice**).
Component Bureau	The CyberScope value for a FISMA reporting entity within the **Reporting Component** (e.g., **Justice Management Division**).

Option	Description
Enclaves	The CyberScope value for an enclave associated with the **Reporting Component** or **Component Bureau**.

DISA Options

The following table describes the additional options to configure when configuring a **DISA** attribute.

Option	Description
Owning Unit	
Name	(Required) The Cyber Operational Attributes Management System (COAMS) fully qualified hierarchy name of the owning organization.
Owning Service	
Name	The COAMS fully qualified hierarchy name of the owning combatant command, service, or agency.
Current AOR	The COAMS fully qualified hierarchy name of the appropriate combatant command area of responsibility (COCOM AOR).
Region	A region for the owning service.
Administration Unit	
Name	The COAMS fully qualified hierarchy name of the administering organization.
Administration POC	
Any required information you need to provide about the administration unit's point of contact	

Option	Description
(POC). **Tip:** Tenable recommends leaving the **Generational Qualifier** option blank.	
CND Service Provider	
Name	The COAMS fully qualified hierarchy name of the Computer Network Defense Service Provider (CNDSP).
Por Managed	(Required) Specifies if the reported assets are centrally managed by a program management office (PMO): **true** or **false**.
System Affiliation	The COAMS **operationalacredit** value that specifies the fully qualified hierarchy name of the system affiliation.
Location	
Tip: Tenable recommends leaving all options blank except the **Street Address**. The **Street Address** specifies the COAMS geolocation area.	

Report Images

In Tenable Security Center, 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.

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.

To filter the **Report Images** page, see Apply a Filter.

Report Image Options

Option	Description
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 • default-watermark = 887x610 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. **Note:** The image size must be set to 300 DPI to prevent image breaks.
Edit	Edit any of the selected image's options, including name, description, type and file.
Detail	View image details, including name, description, date uploaded, last modified, and type.
Delete	Delete the highlighted image.

Filters

You can apply filters on many pages of the Tenable Security Center Director web interface to filter the data displayed on the page.

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).

If you want to save a filter for repeated use, create a query, as described in Queries.

For more information, see:

- Apply a Filter
- Filter Components
- Vulnerability Analysis Filter Components
- Host Asset Filter Components
- Plugin Filter Components

Apply a Filter

Required Tenable Security Center User Role: Any

You can use filters to narrow the data displayed on specific pages.

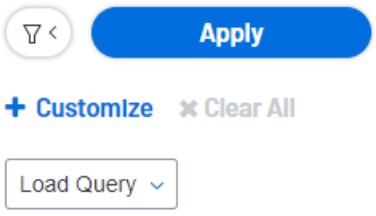
Each filterable page in Tenable Security Center Director has a different set of filter components. On the **Vulnerabilities** page, you can add and remove filter components.

For more information, see Filters and Filter Components.

To filter data:

1. Log in to Tenable Security Center Director via the user interface.
2. Navigate to any page that supports filtering.
3. On the left side of the page, click the ▽ button.

   The filter panel appears.

4. (Optional) To customize the filter components on an analysis page, do the following:

a. Click **Customize**.

   The filter components selection window appears.

b. Select one or more filter component check boxes. For more information about the components supported for your analysis view, see Vulnerability Analysis Filter Components and Host Asset Filter Components.

c. Click **Apply**.

   The filter panel updates to show the filter components you selected.

5. To modify the criteria for a filter component, click the box for the filter component.

   The filter component criteria selection window appears.

6. Modify the filter component criteria.
7. Click **OK**.

   The filter panel updates to show the filter component criteria you modified.

8. Click **Apply**.

   The page updates to reflect the filter you applied.

What to do next:

- (Optional) Save a filter on the **Vulnerabilities** page, **Events** page, and **Mobile** page as a reusable query, as described in Add or Save a Query.

Filter Components

For general information about using filters, see Filters.

Filter Component	Description
Access	The level of object access to include in the filter: • **Manageable** – Shows the objects your user account can modify. For example, set the filter to show only the reports you can edit.

Filter Component	Description
	• **Usable** – Shows the objects your user account can view or use. For example, set the filter to show only the reports you can view.
Actions	The alert actions to include in the filter: **Email**, **Notify**, **Report**, **Scan**, **SysLog**, or **Ticket**. For more information, see Alerts and Alert Actions.
Assignee	The ticket assignees to include in the filter. For more information, see Tickets.
Completion Time	The date range for scan results to include in the filter: • **Explicit** – Choose start and end dates and times to filter for a specific date range. • **Last *x* Minutes** – Filter for the last 15, 20, or 30 minutes. • **Last *x* Hours** – Filter for the last 1, 2, 4, 6, 12, 24, 48, or 72 hours. • **Last *x* Days** – Filter for the last 5, 7, 15, 25, 30, 60, 90, 120, or 180 days. • **Last 12 Months** – Filter for the last year. • **All** – Show all results.
Creator	The ticket creators to include in the filter. For more information, see Tickets.
Data Type	The repository data type to include in the filter: **Agent**, **IPv4**, **IPv6**, or **Mobile**. For more information, see Repositories.
Date	The date range to include in the system log filter (for example, *Oct 2021*). For more information, see System Logs.
Filter By	The type of plugin data to include in the plugin filter. For more information,

Filter Component	Description
	see Vulnerability Analysis Filter Components.
Finish Time	The date range for report results to include in the filter: • **Explicit** – Choose start and end dates and times to filter for a specific date range. • **Last *x* Minutes** – Filter for the last 15, 20, or 30 minutes. • **Last *x* Hours** – Filter for the last 1, 2, 4, 6, 12, 24, 48, or 72 hours. • **Last *x* Days** – Filter for the last 5, 7, 15, 25, 30, 60, 90, 120, or 180 days. • **Last 12 Months** – Filter for the last year. • **All** – Show all results.
Group	The groups to include in the filter. For more information, see Groups.
Host	The name of the host to include in the filter. For more information, see Host.
Initiator	The username for a user who initiated a job to include in the filter. For more information, see Job Queue Events.
Keywords	The keywords to include in the system logs filter (for example, *login*). For more information, see System Logs.
Module	The type of logs to include in the system logs filter. For more information, see System Logs.
Name	The name of the object or user to include in the filter. For example, the name of a Tenable Nessus scanner or the name of a repository.
Organization	The organization to include in the filter. For more information, see

Filter Component	Description
	Organizations.
Owner	The object owners to include in the filter. The object owner is the user who created an object or inherited objects from a deleted user.
Plugin Family	The plugin family to include in the plugin filter.
Plugin Set	The time of the last plugin update for the Tenable Nessus scanner or Tenable Security Center instance: • **Explicit** – Choose start and end dates and times to filter for a specific date range. • **Last *x* Minutes** – Within the last 15, 20, or 30 minutes. • **Last *x* Hours** – Within the last 1, 2, 4, 6, 12, 24, 48, or 72 hours. • **Last *x* Days** – Within the last 5, 7, 15, 25, 30, 60, 90, 120, or 180 days. • **Last 12 Months** – Within the last year. • **All** – Show all results.
Repository	The repository to include in the filter. For more information, see Repositories.
Role	The user roles to include in the filter. For more information, see User Roles.
Scan Policy	The scan policies to include in the filter. For more information, see Scan Policies.
Schedule	The schedules to include in the filter. For more information, see and Report Options.
Severity	The severity to include in the filter. For more information, see CVSS vs.

Filter Component	Description
	VPR.
Status	The statuses to include in the filter.
Tags	The tags to include in the filter. For more information, see Tags.
Tenable Security Center Instance	The Tenable Security Center instance to include in the filter. For more information, see Tenable Security Center Director Deployments.
Timeframe	The date range to include in the notification filter: **Last 24 Hours**, **Last 7 Days**, or **Last 30 Days**.
Type	The object type (for example, **Active** or **Agent** scan results).
Username	The username to include in the filter. For more information, see User Account Options.
Version	The Tenable Nessus version to include in the filter. For more information, see Tenable Nessus Scanners.

Queries

A query is a saved set of filter criteria for vulnerability, event, ticket, alert, or user data. You can apply queries when viewing analysis data to quickly access a consistent, predefined subset of results without reconfiguring filters each time. Tenable Security Center Director includes system-provided queries, and you can create custom queries to fit your environment.

The **Queries** page displays a list of queries available for use. The information on this page 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.

For more information about queries, see:

Manage Queries

Query Options

Manage Queries

Add or Save a Query

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

You can add queries from the **Queries** page or from the **Vulnerabilities** page, **Web App Scanning** page, **Events** page, or **Mobile** 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 **Vulnerabilities** page.

To add a query from the **Queries** page:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Analysis** > **Queries**.

   The **Queries** page appears.
3. At the top of the table, click **Add**.
4. Type a **Name** and **Description**.
5. (Optional) If you want to add a label, type or select a **Label** from the drop-down. For more information, see Labels.
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 ✔ button.

    Tenable Security Center adds the filter component.

12. (Optional) To add other filter components, repeat step 8.
13. Click **Submit**.

    Tenable Security Center Director saves your configuration.

To save a query from an analysis page:

1. Log in to Tenable Security Center via the user interface.
2. Do one of the following to navigate to an analysis page:
   - Click **Analysis** > **Vulnerabilities**
   - Click **Analysis** > **Web App Scanning**
   - Click **Analysis** > **Events**
   - Click **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. Click **Save** > **Save Query**.

   The **Save Query** panel appears.

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 label, type or select a **Label** from the drop-down. For more information, see Labels.

8. Click **Submit**.

   Tenable Security Center Director saves your configuration.

Load a Query

> **Required Tenable Security Center User Role:** Any

You can load queries from any page that supports filtering. For more information, see Queries and Filters.

To load a query:

1. Log in to Tenable Security Center Director via the user interface.
2. Navigate to any page that supports filtering.
3. On the left side of the page, click the filter icon ( ).

   The filter panel appears.
4. Click **Load Query**.
5. Select the query you want to load.
6. Click **Apply**.

   The page updates, filtered by the query you selected.

Edit a Query

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Query Options.

To edit a query:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Analysis** > **Queries**.

   The **Queries** page appears.

3. In the table, right-click the row for the query you want to edit.

   The actions menu appears.

   -or-

   In the table, select the check box for the query you want to edit.

   The available actions appear at the top of the table.

4. Click **Edit**.

   The **Edit Query** page appears.

5. Modify the query options.

6. Click **Submit**.

   Tenable Security Center Director saves the modified query.

Query Options

Queries provide the ability to save custom views of vulnerability, event, ticket, user, and alert data for repeated access.

Option	Description
Name	A name for the query.
Description	A description for the query.
Label	A label for the query. For more information, see see Labels.
Type	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**

Option	Description
	data types, see Ticket-Specific Query Options, User-Specific Query Options, and Alert-Specific Query Options.
Tool	Chooses the analysis tool used by the query.

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 specific user receives a ticket, you could create a query with a ticket filter where the **Assignee** value is the user's name. You could then create an alert to email you when the user receives a ticket. The table below contains a list of the ticket query options.

Option	Description
Name	Ticket name to filter against
Status	Ticket status to filter against.
Classification	The ticket classification to filter against.
Owner	The manager (owner) of the ticket assignee.
Assignee	The ticket assignee to filter against.
Created Timeframe	Ticket creation date/time to filter against. 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.)
Assigned Timeframe	Ticket assigned date/time to filter against. 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.)
Modified	Ticket modified date/time to filter against. Either specify an explicit

Option	Description
Timeframe	timeframe, including the start and end time or choose one of the predefined periods (e.g., last 15 minutes, last hour, etc.)
Resolved Timeframe	Ticket resolution date/time to filter against. 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.)
Closed Timeframe	Ticket closed date/time to filter against. 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.)

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.

Option	Description
First Name	User first name to filter against.
Last Name	User last name to filter against.
Username	Actual username to filter against.
Group	Filter against the group the user(s) belong to.
Role	Filters against users who have the specified role.
Email	Filters against users based on their email address.
Last Login Timeframe	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

Option	Description
	of the predefined periods (e.g., last 15 minutes, last hour, etc.).
Account State	Filters against the user account state (locked vs. unlocked).

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 you want a report, dashboard element, or conditional alert after the specified alert filter conditions have been met. For example, you can schedule a daily report containing a query of all active alerts and their details.

Option	Description
Name	Filter against alerts with the specified name.
Description	Filter against alerts with the specified description.
State	Choose from **All**, **Triggered**, or **Not Triggered**.
Created Timeframe	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.).
Modified Timeframe	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.).
Last Triggered Timeframe	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.).
Last	Filters against the most recent alert evaluation timeframe specified. Either

Option	Description
Evaluated Timeframe	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.).

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

Tenable Security Center 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 notifications, creating or assigning tickets, remediation scans, launching a report, email notifications, and syslog alerting. Multiple actions can be assigned for each ticket.

For more information, see:

Alert Actions

Tenable Security Center automatically performs *alert actions* when an alert triggers. You can configure the following types of alert actions:

- Assign Ticket
- Email
- Generate Syslog

- Launch Report
- Notify Users

Tip: Use email alerts to interface with third-party ticketing systems by adding variables in the message option.

For more information, see Alerts.

Assign Ticket

When the alert triggers, Tenable Security Center creates a ticket and assigns the ticket to a user. For more information, see Tickets.

Option	Description	Default
Name	(Required) The name of the ticket.	Ticket opened by alert
Description	A description for the ticket.	--
Assignee	(Required) The user who receives the ticket.	--

Email

When the alert triggers, Tenable Security Center sends an email.

Option	Description	Default
Email		
Subject	The alert email subject line.	Email Alert
Message	The body of the email message. You can include the following variables to customize the email: • **Alert ID** – Designated with the variable: %alertID%,	(see description)

this specifies the unique identification number assigned to the alert by Tenable Security Center Director.

- **Alert name** – Designated with the variable: %alertName%, this specifies the name assigned to the alert (for example, “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 the operator used for the count: >=, =, >= or !=
- **Trigger value** – Designated with the variable: %triggerValue%, this specifies the specific threshold value set that triggers the alert.
- **Calculated value** – Designated with the variable: %calculatedValue%, this specifies the actual value that triggered the alert.
- **Alert Name** – Designated with the variable: %alertName%, this specifies the name given to the alert within Tenable Security Center Director.
- **Alert owner** – Designated with the variable: %owner%, this specifies the user that created the alert.
- **Tenable Security Center URL** – Designated with the variable: %url%, this specifies the URL that you use to access Tenable Security Center Director. This is useful where the URL that users use to access

	Tenable Security Center Director differs from the URL known by Tenable Security Center Director.
	
	The following sample email alert 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 Security Center Director** (<a href="%url%">%url%</a>) for more information. This e-mail was automatically generated by **Tenable Security Center Director** as a result of alert <strong>%alertName%</strong> owned by <strong>%owner%</strong>.`
	
	`If you do not wish to receive this email, contact the alert owner.`	

Include Results	When enabled, Tenable Security Center includes the query results that triggered the alert (maximum of 500).	Disabled
Recipients		
Users	The users who receive the alert email. **Tip:** If you delete a user who receives alert emails, the action option for the alert turns red and Tenable Security Center displays a notification to the new alert owner with	--

	the new alert status. To resolve this, update the list of users in the alert email.	
Email Addresses	Specifies additional email addresses to include in the alert email. For multiple recipients, add one email address per line or use a comma-separated list.	--

Generate Syslog

When the alert triggers, Tenable Security Center sends a custom message to a syslog server.

Option	Description	Default
Host	(Required) The host that receives the syslog alert.	--
Port	The UDP port used by the remote syslog server.	514
Severity	The severity level of the syslog messages (**Critical**, **Notice**, or **Warning**).	Critical
Message	(Required) The message Tenable Security Center sends with the syslog alert.	--

Launch Report

When the alert triggers, Tenable Security Center generates a report from an existing report template. For more information, see Reports.

Option	Description	Default
Report Template	(Required) The report template Tenable Security Center uses to generate a report based on the triggered alert data.	--

Notify Users

When the alert triggers, Tenable Security Center displays a notification to the specified users.

Option	Description	Default
Message	(Required) The notification message Tenable Security Center sends when the alert triggers.	--
Users	(Required) The users who receive the notification message.	--

Alert Options

The following options are available when you create or edit an alert in Tenable Security Center Director.

Option	Description
General	
Name	The name of the alert.
Description	A description for the alert.
Schedule	Specifies how often the alert checks for the conditions to be matched: **Minutely**, **Hourly**, **Daily**, **Weekly**, **Monthly**, or **Never**. Select **Never** to create an alert that you trigger manually on demand.
Behavior	Specifies how many times Tenable Security Center performs the alert actions: • **Perform actions only on first trigger** – Tenable Security Center performs the alert actions only the first time the alert conditions match the trigger configuration.

Option	Description
General	
	• **Perform action on every trigger** – Tenable Security Center performs the alert actions every time the alert conditions match the trigger configuration.
Condition	
Type	The type of data to use for the condition: **Vulnerability**, **Event**, or **Ticket**.
Trigger	• **IP Count** – Trigger on vulnerabilities or events whose IP address count matches the given parameters. • **Unique Vulnerability Count** – Trigger an alert when the unique vulnerability count matches the given parameters. This option appears when you select **Vulnerability** for the **Type** option. • **Event Count** – Trigger an alert when the event count matches the given parameters. This option appears when you select **Event** for the **Type** option. • **Port Count** – Trigger an alert when the events or vulnerabilities using a certain port number match the given parameters.
Query	The dataset Tenable Security Center uses to determine if trigger conditions have been met.
Filters	Apply advanced filters to the vulnerability or event data. For more information, see Filters.
Actions	
Add Actions	Specifies the actions that occur when the alter triggers: **Assign Ticket**, **Email**, **Generate Syslog**, **Launch Scan**, **Launch Report**, or **Notify Users**. For more

Option	Description
General	
	information, see Alert Actions.

Manage Alerts

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

Add an Alert

You can configure Tenable Security Center Director to send alerts for vulnerability occurrences.

For more information about the available options for alerts, see Alert Options.

To add an alert:

1. Log in to Tenable Security Center Director via the user interface.
2. In the left navigation, click **Workflow** > **Alerts**.

   The **Alerts** page appears.
3. Click **Add**.

   The **Add Alert** page appears.
4. In the **Name** box, type a name.
5. (Optional) In the **Description** box, type a description.
6. (Optional) Click the **Schedule** field to select the frequency of alerts, time, timezone, and whether to repeat sending alerts at the specified time.
7. (Optional) In the **Behavior** drop-down box, select the condition you want to trigger the alert. The default is **Perform actions only on first trigger**.
8. (Optional) In the **Type** drop-down box, select the data type for the condition.

9. In the **Trigger** drop-down box, select the trigger for the alerts.
10. (Optional) In the **Query** drop-down box, select the dataset to compare with the trigger condition.
11. (Optional) Click **Add Filter**and provide the details of the selected filter.
12. Click **Add Actions** to specify an action that occurs when the alert triggers. For more information, see Alert Actions.
13. Click **Submit**.

    Tenable Security Center Director creates the alert.

View Alert Details

You can view the summary details of an alert with the name, behavior, condition applied, status, created date, owner, and ID.

To view the details of an alert:

1. Log in to Tenable Security Center via the user interface.
2. Click **Workflow** > **Alerts**.

   The **Alerts** page appears.
3. In the table, right-click the row for the alert you want to view.

   The actions menu appears.

   -or-

   In the table, select the check box for the alert you want to view.

   The available actions appear at the top of the table.
4. Click **View**.

   The **View Alert** page appears. For more information about the following fields, see Alert Options.

Section	Action
Options drop-down box	• To edit the alert, click **Edit**. For more information, see Edit an Alert. • To delete the alert, click **Delete**. For more information, see Delete an Alert.
General	View general information about the alert. • **Name** – Alert name. • **Description** – Descriptive text for the alert. • **Schedule** – The schedule for how often the alert checks for matching conditions. • **Behavior** – The setting for how the alert behaves once it is triggered. • **Last Evaluated** – The date on which the alert was last evaluated. • **Last Triggered** – The date on which the alert was last triggered. • **Status** – The status of the alert. • **Created** – The date on which the alert was created. • **Last Modified** – The date on which the alert was last modified. • **Owner** – The user who created or owns the alert. • **Group** – The group associated with the **Owner**. • **ID** – The unique identifier of the alert.
Condition	View the conditions specified for the alert: • **Type** – The type of the alert. For example, vulnerability, event, or ticket. • **Trigger** – The condition that triggers the alert. For example, IP count, unique vulnerability/event count, or port count.

Section	Action
	• **Query** – The dataset to which the trigger condition is compared. • **Filters** – The filters added for vulnerability or event data.
Actions	The actions performed once the alert is triggered.

Edit an Alert

For more information, see Alert Options.

To edit an alert:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Workflow** > **Alerts**.

   The **Alerts** page appears.
3. In the table, right-click the row for the alert you want to edit.

   The actions menu appears.

   -or-

   In the table, select the check box for the alert you want to edit.

   The available actions appear at the top of the table.
4. Click **More** > **Edit**.

   The **Edit Alert** page appears.
5. Modify the alert options.
6. Click **Submit**.

   Tenable Security Center Director saves the modified alert.

Evaluate an Alert

You can submit an alert for evaluation to test whether the alert has met the configured time criteria or not.

To evaluate an alert:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Workflow** > **Alerts**.

   The **Alerts** page appears.
3. In the table, right-click the row for the alert you want to evaluate.

   The actions menu appears.

   -or-

   In the table, select the check box for the alert you want to evaluate.

   The available actions appear at the top of the table.
4. Click **Evaluate**.

   The alert is submitted for evaluation.

   Tenable Security Center Director returns the evaluation results for the alert.

Delete an Alert

To delete an alert:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Workflow** > **Alerts**.

   The **Alerts** page appears.
3. In the table, right-click the row for the alert you want to delete.

   The actions menu appears.

   -or-

   In the table, select the check box for the alert you want to delete.

   The available actions appear at the top of the table.
4. At the top of the table, click **More** > **Delete**.

   A confirmation window appears.

5. Click **Delete**.

   Tenable Security Center Director deletes the alert.

Tickets

> **Note:** Ticketing in Tenable Security Center Director will be deprecated in a future release. Please review the Integrations documentation for options on integrating Tenable Security Center Director with external ticketing systems.

In Tenable Security Center Director, you can create tickets manually or automatically using the Alerts feature. This section describes how to manage your tickets.

For more information, see:

Manage Tickets

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

> **Note:** Ticketing in Tenable Security Center Director will be deprecated in a future release. Please review the Integrations documentation for options on integrating Tenable Security Center Director with external ticketing systems.

Open a Ticket

You can use tickets within Tenable Security Center 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 Ticket Options.

To open a ticket from an analysis page:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Analysis** > **Vulnerabilities**.

The Vulnerabilities appears.

3. From the toolbar, click **More** > **Open Ticket**.

   The **Open Ticket** pane appears.

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. Click **Submit**.

   Tenable Security Center Director creates the ticket.

To open a ticket from the **Tickets** page:

1. Log in to Tenable Security Center 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 Security Center Director creates the ticket.

View Ticket Details

You can view the summary details of a ticket with the name, status, creator, assignee, history, queries, description, and ticket notes.

Before you begin:

- Add a ticket, as described in Open a Ticket.

To view a ticket:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Workflow** > **Tickets**.

   The **Tickets** page appears.
3. In the table, right-click the row for the ticket you want to view.

   The actions menu appears.

   -or-

   In the table, select the check box for the ticket you want to view.

   The available actions appear at the top of the table.
4. Click **View**.

   The **View Ticket** page appears. For more information, see Ticket Options.

Section	Action
Options drop-down box	• To edit the ticket, click **Edit**. For more information, see Edit a Ticket.
General	View general information about the ticket. • **Name** – The ticket name. • **Description** – The ticket description. • **Notes** – The notes added for the ticket. • **Status** – The status of the ticket.

Section	Action
	• **Assignee** – The user assigned to the ticket. • **Classification** – The classification selected for the ticket. • **Created** – The date on which the ticket was created. • **Last Modified** – The date on which the ticket was last modified. • **Owner** – The user who created or owns the ticket. • **Group** – The group associated with the **Owner**. • **ID** – The unique identifier of the ticket.
Query Views	The query added to help provide context for coming up with a resolution.

Edit a Ticket

Before you begin:

- Add a ticket, as described in Open a Ticket.

To edit a ticket:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Workflow** > **Tickets**.

   The **Tickets** page appears.
3. In the table, right-click the row for the ticket you want to edit.

   The actions menu appears.

   -or-

   In the table, select the check box for the ticket you want to edit.

   The available actions appear at the top of the table.

4. Click **More** > **Edit**.

   The **Edit Ticket** page appears.

5. Modify the ticket options. For more information, see Ticket Options.
6. Click **Submit**.

   Tenable Security Center Director saves your configuration.

Resolve and Close a Ticket

When a ticket is mitigated, you can change the ticket status to **Resolved**. Once the ticket is resolved, you can change the status to **Closed**. Tickets in the **Resolved** or **Closed** state can always be reopened as needed.

Before you begin:

- Add a ticket, as described in Open a Ticket.

To resolve a ticket:

1. Log in to Tenable Security Center Director via the user interface.
2. Click **Workflow** > **Tickets**.

   The **Tickets** page appears.

3. In the table, right-click the row for the ticket you want to resolve.

   The actions menu appears.

   -or-

   In the table, select the check box for the ticket you want to resolve.

   The available actions appear at the top of the table.

4. Click **Resolve**.

   The **Resolve Ticket** page appears.

5. Change the status to **Resolved**. Optionally, you can add notes to provide details of the resolution.

6. Click **Submit**.
7. To close the ticket, click the resolved ticket name and change the status to **Closed**.

Tenable Security Center Director updates the ticket status. Resolved tickets still show up in your ticket queue with an **Active** status. Closing a ticket removes the ticket from the **Active** status filter view, but does not provide the option to add notes similar to editing a ticket.

Ticket Options

> **Note:** Ticketing in Tenable Security Center Director will be deprecated in a future release. Please review the Integrations documentation for options on integrating Tenable Security Center Director with external ticketing systems.

The following options are available when you create or edit a ticket in Tenable Security Center Director.

Option	Description
General	
Name	Name assigned to the ticket.
Description	Descriptive text for the ticket.
Notes	Notes for the ticket assignee.
Assignee	User that the ticket is assigned to. **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.
Status (Available during edit)	The following ticket statuses become available after a ticket has been created and are available from the **Edit Ticket** page: • **Assigned**

Option	Description
	• **Resolved** • **More Information** • **Not Applicable** • **Duplicate** • **Closed**
Classification	The ticket classification: **Information**, **Configuration**, **Patch**, **Disable**, **Firewall**, **Schedule**, **IDS**, **Accept Risk**, **Recast Risk**, **Re-scan Request**, **False Positive**, **System Probe**, **External Probe**, **Investigation Needed**, **Compromised System**, **Virus Incident**, **Bad Credentials**, **Unauthorized Software**, **Unauthorized System**, **Unauthorized User**, and **Other**.
Query Views	
Add Query View	Click to choose a query for the ticket assignee to help provide context for coming up with a resolution.

Additional Resources

The topics in this section offer guidance in areas related to Tenable Security Center Director.

- Start, Stop, or Restart Tenable Security Center Director
- License Declarations
- Encryption Strength
- File and Process Allow List
- Offline Plugin and Feed Updates for Tenable Security Center Director
- Troubleshooting

Start, Stop, or Restart Tenable Security Center Director

> **Required Tenable Security Center User Role:** Root user

When Tenable Security Center is installed, the required services are started by default.

To change the status of Tenable Security Center Director:

1. Log in to Tenable Security Center Director via the command line interface (CLI).
2. In the CLI in Tenable Security Center Director, run the following command to check the status of your Tenable Security Center Director:

   ```
   # service SecurityCenter status
   ```

   The system indicates whether Tenable Security Center Director is running or stopped.
3. Run one of the following commands to change the status of your Tenable Security Center Director:

- To start Tenable Security Center Director, run:

```
# /bin/systemctl start SecurityCenter
```

- To stop Tenable Security Center Director, run:

```
# /bin/systemctl stop SecurityCenter
```

- To restart Tenable Security Center Director, run:

```
# /bin/systemctl restart SecurityCenter
```

4. If you are running Tenable Security Center Director 6.5.x or later with a managed PostgreSQL database on the same server, then run the following commands to start and stop the PostgreSQL database:

   - To start the PostgreSQL database, run:

```
# su - tns -c "/opt/sc/support/bin/pg_ctl -D /opt/sc/data/postgresql/ -l
/opt/sc/admin/logs/postgresql.log start"
```

   - To stop the PostgreSQL database, run:

```
# su - tns -c "/opt/sc/support/bin/pg_ctl -D /opt/sc/data/postgresql/ stop"
```

Note: These commands assume the install path for the PostgreSQL database is `/opt/sc/`. Replace `/opt/sc/` with your install path if necessary. For more information about managed PostgreSQL databases, see Connect an External PostgreSQL Server.

License Declarations

Tenable Security Center Director's Software License Agreement can be found on Tenable Security Center Director in the `/opt/sc/docs` directory.

For a list of third-party software packages that Tenable utilizes with Tenable Security Center Director, see Tenable Third-Party License Declarations.

Encryption Strength

Tenable Security Center Director uses the following default encryption for storage and communications.

Function	Encryption
Storing TNS user account passwords	SHA-512 and the PBKDF2 function
Storing user and service accounts for scan credentials, as described in Credentials.	AES-256-CBC
Storing scan data, as described in Repositories.	None

Communications between Tenable Security Center and clients (Tenable Security Center users).	The server negotiates the strongest cipher suite supported by both the server and the client.
	
	Note: When FIPS mode is enabled, Tenable Security Center restricts TLS connections to FIPS 140-3 compliant cipher suites and key exchange groups only (NIST-approved curves: P-256, P-384, P-521).
	
	• TLS 1.3
	  • TLS_AES_256_GCM_SHA384
	  • TLS_CHACHA20_POLY1305_SHA256

Function	Encryption
	• TLS_AES_128_GCM_SHA256 • TLS 1.2 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_256_CCM • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA For more information about strong encryption, see Configure SSL/TLS Strong Encryption.
Communications between Tenable Security Center and the Tenable product registration server.	TLS 1.2 with ECDHE-RSA-AES256-GCM-SHA384
Communications between Tenable Security Center and the Tenable plugin update server.	TLS 1.2 with ECDHE-RSA-AES256-GCM-SHA384
Communications	TLS 1.3 with the strongest encryption method supported by

Function	Encryption
between Tenable Security Center and: • Tenable Nessus or Tenable Nessus Manager • Tenable One Vulnerability Management • Tenable Network Monitor	Tenable Security Center 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.
Synchronizations between Tenable Security Center and Tenable One Vulnerability Management for Tenable Lumin.	TLS 1.2

Configure SSL/TLS Strong Encryption

You can configure SSL/TLS strong encryption for Tenable Security Center Director-client communications to meet the security needs of your organization. For more information about Tenable Security Center encryption, see Encryption Strength.

Note: The `sslciphers.conf` file is an Apache-type configuration file that uses OpenSSL-formatted ciphers.

To configure SSL/TLS strong encryptions for Tenable Security Center Director communications:

1. Open the `/opt/sc/support/conf/sslciphers.conf` file in a text editor.

   Note: Before making changes, create a backup copy of `sslciphers.conf` so you can restore the original configuration if needed.

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

   ```
   SSLCipherSuite <cipher you want to use for SSL/TLS encryption>
   ```

   For example:

   ```
   # SSL Ciphers
   SSLProtocol ALL -SSLv2 -SSLv3
   SSLHonorCipherOrder On
   SSLCompression off
   SSLCipherSuite ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-
   AES256-SHA384:ECDHE-RSA-AES256-GCM-SHA384
   ```

3. Restart Tenable Security Center Director, as described in Start, Stop, or Restart Tenable Security Center Director.

   Tenable Security Center 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.

File and Process Allow List

If you use third-party endpoint security products such as anti-virus applications and host-based intrusion and prevention systems, Tenable recommends adding Tenable Security Center Director to the allow list.

If you configured supporting resources for Tenable Security Center Director, see the product documentation for each resource you added for more file and process allow list information. For more information about supporting resources in Tenable Security Center Director, see Resources.

Tenable recommends allowing the following Tenable Security Center Director files and processes.

Allow List
Files
/opt/sc/*
Processes
/opt/sc/bin/*
/opt/sc/src/*
/opt/sc/support/bin/*
/opt/sc/www/*

Asset Tracking in Tenable Security Center Director

Assets in Tenable Security Center Director are tracked by several attributes, depending on the repository and scan configuration of the sensors that identify the assets.

- Imported assets are tracked by asset attribute.
- IP assets are tracked by IP address.
- Tenable Agent assets are tracked by agent UUID.

- Tenable One OT Exposure assets are tracked by Tenable One OT Exposure UUID. For more information about viewing Tenable One OT Exposure data in Tenable Security Center, see Tenable One OT Exposure Instances.

When you import asset data, if Tenable Security Center Director cannot find an existing asset that matches the imported host, the asset is added to Tenable Security Center Director as a new asset.

For more information about asset repositories in Tenable Security Center Director, see Asset Repositories.

Imported Assets

The following identification attributes (IA) are considered in determining whether or not an imported asset matches an existing one, in descending order of priority:

1. Tenable UUID (from credentialed scans of managed hosts, Tenable Agents, or imported Tenable One OT Exposure data)
2. BIOS UUID
3. MAC Address
4. NetBIOS Name
5. Fully Qualified Domain Name (FQDN)
6. IP Address (IPv4 and IPv6)

Similar to Tenable One Vulnerability Management, Tenable Security Center Director verifies that there are no conflicting higher priority attributes when it finds a match. For example, if there is a MAC Address match, but the Tenable UUID is different, the assets will not merge. When a unique asset is discovered, the following informational message will appear in `/opt/sc/admin/logs/YYYYMM.log` (`sc-logs.txt` in a Tenable Security Center Director debug zip).

```
Scan Result #<Job ID> - <IP Address or Agent UUID> did not match any existing assets
```

Possible root causes for duplicate assets include, but are not limited to:

- different scan types for the same asset, such as Agent scans and non-credentialed Tenable Nessus scans or, similarly, credentialed Tenable Nessus scans with the **Create unique identifier on hosts scanned using credentials** (host_tagging) setting disabled in the Advanced settings of the scan policy. While Agent scans have access to the local Tenable UUID, the same is not true for a non-credentialed or equivalent scan. If an asset was duplicated as a result of a non-credentialed or equivalent scan after a credentialed one, the assets will not merge until the next credentialed or equivalent scan.
- different network interfaces of an asset scanned in one or more non-credentialed scans. Because each network interface is associated with a different MAC Address, and the Tenable UUID cannot be accessed in a non-credentialed scan, a unique asset will be created for each network interface.

For more information about imported assets, see Asset Repositories.

IPv4 and IPv6 Assets

If the **Track hosts which have been issued new IP address** setting is enabled (default), assets are tracked using the following IAs in this order:

1. Tenable UUID (from credentialed scans of managed hosts, Tenable Agents, or imported Tenable One OT Exposure data)
2. BIOS UUID
3. MAC Address
4. NetBIOS Name
5. Fully Qualified Domain Name (FQDN)
6. IP Address (IPv4 and IPv6)

If the **Track hosts which have been issued new IP address** setting is disabled, assets are tracked only by IP address. When you import a scan result for an IP address not already in the repository, Tenable Security Center Director creates a new asset for that IP and does not modify existing assets.

During scan import, Tenable Security Center Director checks the targeted repository for the scan job for the above listed IAs.

- If the IP has the attributes mentioned above, Tenable Security Center Director migrates all of the vulnerabilities in the cumulative results to the IP seen in the scan result.
- If the IP does not have any of the attributes mentioned above, Tenable Security Center Director considers this a new asset.
- Once a match has been made, Tenable Security Center Director does not search for more matches.

For example, if Tenable Security Center Director does not match a DNS name, but it does match a NetBIOS name, the system does not check the Agent UUID or MAC address.

> **Note:** The **Track hosts which have been issued new IP address** setting is in the Advanced settings section, and is enabled by default in Active Scans. Tenable recommends that networks using DHCP enable this setting to properly track hosts.

For more information about IPv4 and IPv6 assets, see Asset Repositories.

Agent Assets

Agent assets are tracked by UUID, because all agent assets have UUIDs.

> **Note:** The Tenable UUID assigned during credentialed scans and the UUID assigned to Tenable Agents are stored in the same location on the host: `/etc/tenable_tag` on Linux, or the registry at `HKLM\SOFTWARE\Tenable\TAG` on Windows. When a credentialed scan runs with the **Create unique identifier on hosts scanned using credentials** setting enabled, Tenable Nessus reads this value if it exists (written by a previously installed agent) or writes a new one if it does not. This means an asset scanned by both a Tenable Agent and a credentialed Tenable Nessus scan shares the same Tenable UUID, allowing Tenable Security Center Director to correctly identify it as a single asset rather than creating duplicates.

For more information about agent assets, see Asset Repositories.

Offline Plugin and Feed Updates for Tenable Security Center Director

You can perform offline plugin updates and feed updates in air-gapped Tenable Security Center Director environments.

- Perform an Offline Nessus Plugin Update
- Perform an Offline Tenable Network Monitor Plugin Update
- Perform an Offline Tenable Security Center Feed Update

For general information about best practices in air-gapped environments, see Considerations for Air-Gapped Environments.

Note: Update your active plugins before you update the Tenable Security Center feed. Updating active plugins first ensures proper VPR mapping. If you update the Tenable Security Center feed before updating active plugins, newly supported plugins may not yet exist in your active plugin set, which can result in incomplete VPR data.

Perform an Offline Nessus Plugin Update

Required Tenable Security Center User Role: Administrator

Note: You can also download offline feed files directly from connect.tenable.com. In Tenable Connect, go to **Account Management** > **Products** > **Security Center** > **Manage Product** > **View Feed Credentials** and use the provided links to download the feed files. This method does not require the offline registration steps described below.

Before you begin:

- Install a temporary Tenable Nessus scanner on the same host as Tenable Security Center Director. You will use this temporary Tenable Nessus scanner to generate a challenge code for offline Tenable Security Center registration. Do not start or otherwise configure the temporary Tenable Nessus scanner.

To perform an offline Tenable Nessus plugin update:

1. In the command line interface (CLI), run the following command to prevent the Tenable Nessus scanner from starting automatically upon restarting the system:

   ```
   /usr/bin/systemctl disable nessusd
   ```

2. Run the following command and save the challenge string that is displayed:

   ```
   # /opt/nessus/sbin/nessuscli fetch --challenge
   ```

3. In your browser, navigate to https://plugins.nessus.org/offline.php.

   Note: Do not click **here**, even if you have a newer version of Tenable Nessus installed. You cannot use the https://plugins.nessus.org/v2/offline.php page for Tenable Security Center downloads.

4. Paste the challenge string from Step 2 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.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.tar.gz`.
9. Verify the file using the SHA256 checksum, as described in the knowledge base article.
10. Save the `sc-plugins.tar.gz` on the system used to access your Tenable Security Center Director web interface.
11. Log in to Tenable Security Center 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.tar.gz` file.

16. Click **Submit**.

    After several minutes, the plugin update finishes and the page updates the **Last Updated** date and time.

What to do next:

- If you installed a temporary Tenable Nessus scanner on the same host as Tenable Security Center Director, uninstall the Tenable Nessus scanner.

Perform an Offline Tenable Network Monitor Plugin Update

Required Tenable Security Center User Role: Administrator

Before you begin:

- Install a temporary Tenable Nessus scanner on the same host as Tenable Security Center Director. You will use this temporary Tenable Nessus scanner to generate a challenge code for offline Tenable Security Center registration. Do not start or otherwise configure the temporary Tenable Nessus scanner.

To perform an offline Tenable Network Monitor plugin update:

1. In the command line interface (CLI), run the following command to prevent the Tenable Network Monitor scanner from starting automatically upon restarting the system:

```
/usr/bin/systemctl disable nnm
```

2. Run the following command and save the challenge string that is displayed:

```
# /opt/nnm/bin/nnm --challenge
```

3. In your browser, navigate to the Tenable Network Monitor 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 Security Center 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 SHA256 checksum, as described in the knowledge base article.
10. Save the `sc-passive.tar.gz` on the system used to access your Tenable Security Center GUI.

    Note: Access the Tenable Network Monitor feed setting and change the activation from offline to Tenable Security Center Director.
11. Log in to Tenable Security Center 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.

What to do next:

- If you installed a temporary Tenable Nessus scanner on the same host as Tenable Security Center Director, uninstall the Tenable Nessus scanner.

Perform an Offline Tenable Security Center Feed Update

Required Tenable Security Center User Role: Administrator

Note: If you already performed a Tenable Nessus offline plugin update, start at step 7.

Note: You can also download offline feed files directly from connect.tenable.com. In Tenable Connect, go to **Account Management** > **Products** > **Security Center** > **Manage Product** > **View Feed Credentials** and use the provided links to download the feed files. This method does not require the offline registration steps described below.

Before you begin:

- Install a temporary Tenable Nessus scanner on the same host as Tenable Security Center Director. You will use this temporary Tenable Nessus scanner to generate a challenge code for offline Tenable Security Center registration. Do not start or otherwise configure the temporary Tenable Nessus scanner.

To perform an offline Tenable Security Center feed update:

1. In the command line interface (CLI), run the following command to prevent the Tenable Nessus scanner from starting automatically upon restarting the system:

   ```
   /usr/bin/systemctl disable nessusd
   ```

2. To obtain the challenge code for an offline Tenable Security Center registration, do one of the following:

- If you installed Tenable Security Center in an environment other than Tenable Core, run the following command and save the challenge code:

```
# /opt/nessus/sbin/nessuscli fetch --challenge
```

3. In your browser, navigate to https://plugins-customers.nessus.org/offline.php.
4. Paste the challenge code from Step 2 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.
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 link 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 SHA256 checksum, as described in the knowledge base article.
11. Save the `SecurityCenterFeed48.tar.gz` on the system used to access your Tenable Security Center Director GUI.
12. Log in to Tenable Security Center 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 Security Center 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.

What to do next:

- If you installed a temporary Tenable Nessus scanner on the same host as Tenable Security Center Director, uninstall the Tenable Nessus scanner.

Migrate Data Between PostgreSQL Implementations

If you want to migrate Tenable Security Center Director data between PostgreSQL implementations, Tenable offers a script to simplify the process.

The script is supported for the following use cases:

- Existing Tenable Security Center Director installs that are licensed and configured. For new installs, follow the directions in Connect an External PostgreSQL Server.
- Migrating from an internal to an external PostgreSQL.
- Migrating from an external PostgreSQL version 13 through 16 to an internal or external PostgreSQL version 13 through 17.
- Migrating from an external PostgreSQL version 17 to an external PostgreSQL version 17. In this scenario, the script will only modify the PostgreSQL configuration. You will need to migrate your data manually after running the script.

Note: The following migration paths are not supported:

- Migrating from an external PostgreSQL to an external PostgreSQL of an earlier version. For example, migrating from an external PostgreSQL version 17 to an external PostgreSQL version 16.
- Migrating from an external PostgreSQL version 17 to internal PostgreSQL.

This page includes two sets of instructions:

- Migrate from internal PostgreSQL or PostgreSQL 13 through 16

  Use these steps if you are migrating from an internal PostgreSQL to an external PostgreSQL, or if you are migrating from an external PostgreSQL version 13 through 16 to an internal or external PostgreSQL 13 through 17.

- Migrate from PostgreSQL 17

  Use these steps if you are migrating from an external PostgreSQL 17 to an external PostgreSQL 17.

Note: In the following instructions, the *source server* is the PostgreSQL that you are migrating data from, and the *destination server* is the PostgreSQL that you are migrating data to.

Before you begin

- The destination PostgreSQL must be a supported version. For information about supported PostgreSQL versions, see External PostgreSQL Requirements.
- Ensure that both the source PostgreSQL server and the destination PostgreSQL server are currently running.
- On the destination PostgreSQL server, you must have the permission to create a database. If the database is already created, then you must have read and write permissions.

Migrate from internal PostgreSQL or PostgreSQL 13 through 16

Migrate data from an internal PostgreSQL or a PostgreSQL version 13 through 16 implementation

1. Stop Tenable Security Center Director with the following command:

   ```
   # /bin/systemctl stop SecurityCenter
   ```

2. Check the PostgreSQL status with the following command:

   ```
   /opt/sc/support/bin/pg_ctl status -D /opt/sc/data/postgresql
   ```

3. If the PostgreSQL service is not running, start the service as the `tns` user with the following command:

   Note: You cannot run `pg_ctl` as the `root` user. Run all `pg_ctl` commands as the `tns` user.

   If you are migrating from an external PostgreSQL to the internal PostgreSQL and the internal data directory has not been initialized (for example, you configured the external PostgreSQL when you installed Tenable Security Center Director), initialize the data directory before you start the service:

   ```
   su - tns -c "/opt/sc/support/bin/initdb -D /opt/sc/data/postgresql --encoding=UTF8"
   ```

   ```
   su - tns -c "/opt/sc/support/bin/pg_ctl start -D /opt/sc/data/postgresql/ -l
   /opt/sc/admin/logs/postgresql.log"
   ```

4. Set the environment variables for the destination PostgreSQL server.

   Note: You must set the environment variables with a `root` or `tns` user account. Use the same account to run the script in step 4. If you are using the `tns` user account to run the script, switch to the `tns` user using the command `su - tns`.

5. Run the following script on the server where you have installed Tenable Security Center Director:

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

   The data on the source server is copied to the destination server.

6. Start Tenable Security Center Director with the following command:

   ```
   # /bin/systemctl start SecurityCenter
   ```

7. If you manually started the PostgreSQL service in step 3 and the internal PostgreSQL is not your migration destination, stop the service as the `tns` user with the following command:

```
su - tns -c "/opt/sc/support/bin/pg_ctl stop -D /opt/sc/data/postgresql/"
```

Note: If you are migrating to the internal PostgreSQL, do not stop the service. Tenable Security Center Director uses the internal PostgreSQL after you start Tenable Security Center Director.

Migrate from PostgreSQL 17

Migrate data from a PostgreSQL version 17 implementation

1. Stop Tenable Security Center Director with the following command:

```
# /bin/systemctl stop SecurityCenter
```

2. Set the environment variables for the destination PostgreSQL server.

Note: You must set the environment variables with a `root` or `tns` user account. Use the same account to run the script in step 4.

3. Run the following script on the server where you have installed Tenable Security Center Director:

```
/opt/sc/support/bin/php /opt/sc/src/tools/movePostgresDB.php config-only
```

4. Log in to your destination server and clean any data added by default.
    1. Log in to your destination PostgreSQL server with the following command, where *<username>* is your PostgreSQL username:

```
sudo su - <username>
```

2. Clear data by running the following SQL commands in the PostgreSQL terminal:

```
CREATE OR REPLACE FUNCTION truncate_public_schema_tables()
RETURNS void AS $$
DECLARE
    table_name text;
BEGIN
    FOR table_name IN (SELECT tablename FROM pg_tables WHERE schemaname = 'public') LOOP
        EXECUTE 'TRUNCATE TABLE public.\"' || table_name || '\" CASCADE;';
    END LOOP;
END;
$$ LANGUAGE plpgsql;

SELECT truncate_public_schema_tables();

DROP FUNCTION IF EXISTS truncate_public_schema_tables();
```

5. Migrate your data from the source server to the destination server.
    a. Log in to your source PostgreSQL server with the following command, where *<username>* is your PostgreSQL username:

```
sudo su - <username>
```

    b. Dump the contents of the source server to a directory with the following command, where *<dbname>* is the name of the source PostgreSQL server, and *<backup_name>* is the name of the backup file:

```
pg_dump <dbname> -O -a -F d -f <backup_name> -j 5 2>&1
```

    c. Restore the dumped contents to the destination server with the following command, where *<admin:admin@[IP address of new PG]:port/dbname>* is the path to the destination PostgreSQL server, and *<backup_name>* is the name of the backup file you created in the previous step:

```
pg_restore -d postgresql://<admin:admin@[IP address of new PG]:port/dbname> -O -a -F d
<backup_name> -j 5 2>&1
```

The data on the source server is copied to the destination server.

6. Start Tenable Security Center Director with the following command:

```
# /bin/systemctl start SecurityCenter
```

Troubleshooting

This troubleshooting section covers some of the common issues encountered with Tenable Security Center Director.

General Tenable Security Center Director Troubleshooting

General Tenable Security Center Director Troubleshooting

Tenable Security Center 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 Security Center 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 Security Center Director host:

```
# df

Filesystem                      1K-blocks     Used       Available     Use%
Mounted on
/dev/mapper/VolGroup00-LogVol00    8506784       8506784    0             100%
```

```
/
/dev/sda1                         101086        24455      71412         26%
/boot
tmpfs                             1037732       0          1037732       0%
/dev/shm
```

4. If there is not enough drive space, recover sufficient space and restart the Tenable Security Center Director service:

```
# df

Filesystem                        1K-blocks     Used       Available     Use%
Mounted on
/dev/mapper/VolGroup00-LogVol00   8506784       6816420    1251276       85%
/
/dev/sda1                         101086        24455      71412         26%
/boot
tmpfs                             1037732       0          1037732       0%
/dev/shm

# service SecurityCenter restart

Shutting down SecurityCenter services:                     [  OK  ]
Starting SecurityCenter services:                          [  OK  ]
#
```

Locked out of all Tenable Security Center 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.