



Tenable.sc 5.16.x User Guide

Last Revised: October 12, 2021



Table of Contents

Welcome to Tenable.sc	17
Get Started With Tenable.sc	18
Considerations for Air-Gapped Environments	22
Requirements	24
Hardware Requirements	25
Cloud Requirements	28
System Requirements	33
Customize SELinux Enforcing Mode Policies for Tenable.sc	37
Use /dev/random for Random Number Data Generation	38
License Requirements	39
Apply a New License	41
Update an Existing License	42
Tenable.sc CV License Expiration	44
Port Requirements	45
Web Browser Requirements	46
Tenable Integrated Product Compatibility	47
Large Enterprise Deployments	48
Installation and Upgrade	49
Before You Install	50
Install Tenable.sc	52
Quick Setup	54
Before You Upgrade	59



Upgrade Tenable.sc	61
Restore Custom SSL Certificates	63
Uninstall Tenable.sc	65
User Access	66
Log In to the Web Interface	67
Log in to the Web Interface via SSL Client Certificate	69
User Roles	72
Create a User Role	77
Edit a User Role	78
View User Role Details	80
Delete a User Role	82
Organizations and Groups	83
Organizations	84
Add an Organization	88
View Organization Details	89
Delete an Organization	91
Groups	92
Add a Group	94
View Group Details	95
Delete a Group	96
User Accounts	97
Add a TNS-Authenticated User	101
Add an LDAP-Authenticated User	103
Add a SAML-Authenticated User	106



Manage User Accounts	109
Edit Your User Account	110
View User Details	111
Delete a User	113
Linked User Accounts	115
Add a Linked User	116
Switch to a Linked User Account	118
Edit a Linked User Account	119
Delete a Linked User Account	120
Custom Group Permissions	122
Generate API Keys	125
Delete API Keys	127
LDAP Authentication	128
Add an LDAP Server	131
Delete an LDAP Server	132
LDAP Servers with Multiple OUs	133
SAML Authentication	136
Configure SAML Authentication Automatically via the User Interface	139
Configure SAML Authentication Manually via the User Interface	141
Configure SAML Authentication via the SimpleSAML Module	143
SAML User Provisioning	147
Configure SAML User Provisioning	148
SAML Authentication XML Configuration Examples	150
Certificate Authentication	155



Configure Tenable.sc to Allow SSL Client Certificate Authentication	156
Configure a CRL in Tenable.sc	158
Configure OCSP Validation in Tenable.sc	162
Certificates and Certificate Authorities in Tenable.sc	164
Tenable.sc Server Certificates	165
Upload a Server Certificate for Tenable.sc	166
Regenerate the Tenable.sc Server Certificate	168
Trust a Custom CA	170
System Settings	171
Configuration Settings	172
Edit Plugin and Feed Settings and Schedules	183
Configure Plugin Text Translation	185
API Key Authentication	186
Enable API Key Authentication	187
Disable API Key Authentication	188
Enable Picture in Picture	189
Disable Picture in Picture	190
Lumin Data	191
View Lumin Metrics	192
View Lumin Data Synchronization Logs	194
Diagnostics Settings	197
Generate a Diagnostics File	199
Enable Touch Debugging	200
Disable Touch Debugging	201



Job Queue Events	202
System Logs	203
View System Logs	204
Publishing Sites Settings	205
Keys Settings	206
Add a Key	207
Delete a Key	208
Download the Tenable.sc SSH Key	209
Username Menu Settings	210
Custom Plugin Packages for NASL and CA Certificate Upload	213
Create the Custom Plugin Package	216
Upload the Custom Plugin Package	217
Troubleshooting Issues with the custom_CA.inc File	218
Backup and Restore	220
Perform a Backup	221
Restore a Backup	223
Lumin Synchronization	225
Plan Your Lumin Synchronization	226
Repository Overlap	229
Configure Lumin Synchronization	230
View Lumin Synchronization Status	235
Disable Lumin Synchronization	237
Configure Scans	238
Scanning Overview	239



Resources	241
Nessus Scanners	242
Add a Nessus Scanner	246
Add a Tenable.io Scanner	248
Nessus Scanner Statuses	251
Manage Nessus Scanners	254
View Your Nessus Scanners	255
View Details for a Nessus Scanner	257
View Nessus Instances in Tenable.sc	259
Download Nessus Scanner Logs	260
Delete a Nessus Scanner	262
Nessus Network Monitor Instances	263
Add an NNM Instance	265
View Your NNM Instances	267
NNM Instance Settings	268
Log Correlation Engines	270
Add a Log Correlation Engine Server	272
Log Correlation Engine Clients	274
Log Correlation Engine Client Policies	275
Tenable.ot Instances	276
Repositories	277
Add a Repository	278
Manage Repositories	280
View Your Repositories	282



View Repository Details	283
Export a Repository	286
Import a Repository	288
Delete a Repository	289
Local Repositories	290
IPv4/IPv6 Repositories	291
Mobile Repositories	293
Agent Repositories	301
External Repositories	303
Offline Repositories	304
Remote Repositories	307
Tiered Remote Repositories	309
Configure Tiered Remote Repositories	310
Active Scans	311
Add an Active Scan	313
Manage Active Scans	315
Start or Pause a Scan	317
Suspend or Resume a Scheduled Active Scan	318
Run a Diagnostic Scan	319
Active Scan Settings	321
Launch a Remediation Scan	328
Active Scan Objects	330
Assets	332
Add a Template-Based Asset	341



Add a Custom Asset	343
View Asset Details	344
Credentials	346
Add Credentials	347
API Gateway Credentials	349
Database Credentials	351
Database Credentials Authentication Method Settings	358
SNMP Credentials	367
SSH Credentials	368
Privilege Escalation	379
Windows Credentials	381
Audit Files	392
Add a Template-Based Audit File	394
Add a Custom Audit File	396
Manage Audit Files	398
Scan Zones	400
Add a Scan Zone	403
View Your Scan Zones	404
Edit a Scan Zone	405
Delete a Scan Zone	406
Scan Policies	407
Add a Scan Policy	408
Scan Policy Templates	410
Scan Policy Options	415



Configure Compliance Options	443
Configure Plugin Options	444
Host	447
Miscellaneous	448
Plaintext Authentication	453
Patch Management	457
View Your Scan Policies	466
View Scan Policy Details	467
Edit a Scan Policy	469
Share or Revoke Access to a Scan Policy	470
Export a Scan Policy	471
Import a Scan Policy	473
Copy a Scan Policy	475
Delete a Scan Policy	476
Agent Scanning	477
Agent Scans	479
Add an Agent Scan	480
Manage Agent Scans	482
Start or Pause a Scan	484
Agent Scan Settings	485
Agent Synchronization Jobs	488
Add an Agent Synchronization Job	489
Manage Agent Synchronization Jobs	491
Agent Synchronization Job Settings	493



Blackout Windows	496
Add a Blackout Window	498
Edit a Blackout Window	499
Delete a Blackout Window	500
Tags	501
Add a Tag	502
Remove or Delete a Tag	503
Analyze Data	504
Dashboards	505
View a Dashboard	507
Overview Dashboard	509
LCE Overview Dashboard	511
Set a Dashboard as Your Default Dashboard	512
Add a Template-Based Dashboard	513
Add a Custom Dashboard	515
Dashboard and Component Templates	517
Import a Dashboard	519
Manage Dashboards	520
Edit Settings for a Dashboard	522
Share or Revoke Access to a Dashboard	523
Delete a Dashboard	524
Manage Dashboard Components	525
Add a Template-Based Dashboard Component	527
Add a Custom Dashboard Component	529



Custom Dashboard Component Options	531
Configure a Simple Matrix Dashboard Component	541
Scan Results	546
Scan Result Statuses	547
Manage Scan Results	549
View Scan Results	552
View Scan Result Details	554
Upload Scan Results	557
Solutions Analysis	559
View Solutions	560
View Solution Details	562
Vulnerability Analysis	564
Cumulative vs. Mitigated Vulnerabilities	565
View Cumulative or Mitigated Vulnerabilities	566
CVSS vs. VPR	567
Vulnerability Analysis Tools	571
Vulnerability Analysis Filter Components	577
View Vulnerabilities by Host	590
View Vulnerabilities by Plugin	592
View Vulnerability Instance Details	595
View Host Details	598
View Plugin Details	600
Export Vulnerability Data	602
Event Analysis	603



Event Analysis Tools	607
Event Analysis Filter Components	611
Mobile Analysis	614
Mobile Analysis Filter Components	615
Reports	617
Manage Reports	618
Create a Custom Report	619
Create a Template Report	620
Data Required for Template-Based Reports	623
Report Templates	624
Edit a Report Definition	626
Report Options	627
Edit a Report Outline	635
Add a Custom Chapter to a Report	637
Add a Template Chapter to a Report	638
Add or Edit a Report Element	641
Configure a Grouping Element in a Report	642
Configure a Text Element in a Report	647
Configure a Matrix Element in a Report	650
Configure a Table Element in a Report	653
Configure a Charts Element in a Report	656
Reorder Report Chapters and Elements	660
Manage Filters for a Chapter Report	661
Manage Filter Components for a Single Element	662



Manage Filter Components for Multiple Elements	664
Manage Filter Components for a Non-Chapter Report	666
View a Report Definition	668
Copy a Report Definition	669
Export a Report Definition	670
Import a Report Definition	672
Delete a Report Definition	673
Launch a Report on Demand	674
Add a Report to a Scan	675
Manage Report Results	676
Stop a Running Report	677
Download a Report Result	678
View a Report Result	679
Publish a Report Result	680
Email a Report Result	681
Copy a Report Result	682
View Errors for a Failed Report	683
Delete a Report Result	684
CyberScope and DISA Report Attributes	685
Report Images	688
Assurance Report Cards	689
Add a Template-Based Assurance Report Card	690
Add a Custom Assurance Report Card	692
View Your Assurance Report Cards	693



View Details for an Assurance Report Card	695
Edit an Assurance Report Card	697
Share or Revoke Access to an Assurance Report Card	698
Export an Assurance Report Card	699
Copy an Assurance Report Card	701
Delete an Assurance Report Card	702
Assurance Report Card Options	703
Filters	706
Apply a Filter	707
Queries	713
Add or Save a Query	717
Load a Query	719
Workflow Actions	720
Alerts	721
Alert Actions	723
Tickets	728
Open a Ticket	730
Accept Risk Rules	732
Add an Accept Risk Rule	733
Delete an Accept Risk Rule	734
Recast Risk Rules	735
Add a Recast Risk Rule	736
Delete a Recast Risk Rule	737
Additional Resources	738



Start, Stop, or Restart Tenable.sc	739
License Declarations	740
Encryption Strength	741
Configure SSL/TLS Strong Encryption	743
Configure Tenable.sc for NIAP Compliance	744
File and Process Allow List	746
Manual LCE Key Exchange	747
Manual Nessus SSL Certificate Exchange	750
Overview of Nessus SSL Certificates and Keys	751
Nessus Certificate Configuration for Unix	752
Nessus Certificate Configuration for Windows	762
Offline Tenable.sc Plugin and Feed Updates	767
Perform an Offline Nessus Plugin Update	768
Perform an Offline NNM Plugin Update	770
Perform an Offline Tenable.sc Feed Update	772
Troubleshooting	775
General Tenable.sc Troubleshooting	776
LCE Troubleshooting	778
Nessus Troubleshooting	780
NNM Troubleshooting	782



Welcome to Tenable.sc

This user guide describes how to install, configure, and manage Tenable.sc™ 5.16.x.

Tenable.sc is a comprehensive vulnerability management solution that provides complete visibility into the security posture of your distributed and complex IT infrastructure. Tenable.sc 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.

To get started, see [Get Started With Tenable.sc](#).



Get Started With Tenable.sc

Use the following getting started sequence to configure and mature your Tenable.sc deployment.

1. [Prepare](#)
2. [Install](#)
3. [Configure Scans](#)
4. [Refine](#)
5. [Expand](#)

Prepare

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

- Access Tenable Support and training resources for Tenable.sc, including:
 - the [Tenable Deployment Strategy Planning](#) video
 - the [Tenable University](#) training courses
 - the [Tenable Scan Strategy](#) guide
- Design a deployment plan by identifying your organization's objectives and analyzing your network topology. Consider Tenable-recommended best practices for your environment. For more information about environment requirements, see [Requirements](#). For information about scan types, see [Scanning Overview](#).
- Design an analysis workflow. Identify key stakeholders in your management and operational groups, considering the data you intend to share with each stakeholder.

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

Install

Install Tenable.sc and perform initial configuration.



1. Depending on your environment, [install in your environment](#) or [deploy or install with Tenable Core](#).

For complete information about Tenable Core + Tenable.sc, see the [Tenable Core User Guide](#).

2. Perform quick setup, as described in [Quick Setup](#). You can:
 - Upload licenses
 - Configure one Nessus scanner
 - Configure one NNM scanner (requires a NNM activation license)
 - Configure one LCE server (requires an LCE® activation license)
 - Create one repository
 - Create one organization
 - Configure one LDAP server
 - 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.

3. Configure SMTP settings, as described in [Mail Settings](#).
4. Configure scan zones, as described in [Add a Scan Zone](#).
5. Configure additional repositories, if necessary, as described in [Repositories](#).
6. Configure additional scanners, if necessary, as described in [Nessus Scanners](#), [Nessus Network Monitor Instances](#), and [Log Correlation Engines](#).
7. Configure security settings (e.g., password complexity requirements and custom banners), as described in [Security Settings](#).

Configure Scans



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

1. Configure credentials, as described in [Credentials](#).
2. Create static assets, as described in [Add a Custom Asset](#). For more information about asset types, see [Assets](#).
3. Configure a Host Discovery policy and a Basic Network Scan policy from Tenable-provided scan policy templates, as described in [Add a Scan Policy](#).
4. Configure and run scans for those policies, as described in [Add an Active Scan](#) and [Add an Agent Scan](#).
5. Confirm that the scans can access all areas of your network with no credential issues.
6. Configure NNM scanners, as described in [Nessus Network Monitor Instances](#).
7. When the scans complete, create template-based dashboards and reports, as described in [Dashboards](#) and [Reports](#).

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

Refine

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

- Configure audit files, as described in [Audit Files](#).
- Create additional scan policies, as described in [Add a Scan Policy](#).
- Configure scan blackout windows, as described in [Add a Blackout Window](#).
- Configure groups, as described in [Add a Group](#).
- Create a custom user role, as described in [Create a User Role](#).
- Create additional user accounts and share objects with users, as described in [User Accounts](#).
- Create dynamic assets and combination assets, as described in [Add a Custom Asset](#). For more information about asset types, see [Assets](#).



- Review the plugin update schedule, as described in [Edit Plugin and Feed Settings and Schedules](#). Consider editing the schedules to suit your needs. For example, you may want to schedule plugin and feed updates to run a few hours before your scheduled scans.
- Add queries and use filters, as described in [Add or Save a Query](#) and [Apply a Filter](#).
- Create custom dashboards and reports, as described in [Dashboards](#) and [Reports](#).
- Create Assurance Report Cards (ARCs), as described in [Assurance Report Cards](#).
- Configure alerts, ticketing, accept risk rules, and recast risk rules, 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 and consider revising.
- Review your scan results and scan coverage. You may need to modify your scan configurations to suit your organization's objectives and reach all areas of your network.
- Optimize and operationalize your custom dashboards to meet the needs of individual user account holders.
- Optimize and operationalize your custom reports to prepare them for distribution.
- Consider configuring API integrations, as described in the [Tenable.sc API Guide](#) and the [Tenable.sc API Best Practices Guide](#).
- Consider synchronizing Tenable.sc with Tenable.io Lumin to take advantage of Cyber Exposure features, as described in [Lumin Synchronization](#).



Considerations for Air-Gapped Environments

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

Architecture

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

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

Upgrades and Updates

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

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

After you perform a plugin update or feed update, verify the files as described in the [knowledge base](#) article.

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

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

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



4. Upload the files to Tenable.sc.

- Tenable.sc upgrade: [via the CLI](#).
- Plugin/feed update: [in a browser](#) or [via the API](#).

Nessus Agents

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

For more information, see the [knowledge base](#) article.



Requirements

You can run Tenable.sc in the following environments.

Environment			More Information
Tenable Core	Virtual	VMware	Requirements in the <i>Tenable Core User Guide</i>
		Microsoft Hyper-V	
	Cloud	Amazon Web Services (AWS)	
	Hardware		
Other plat- forms	Cloud	Amazon Web Services (AWS)	Cloud Requirements
	Hardware		Hardware Requirements

For general information about other requirements to run Tenable.sc, see:

- [System Requirements](#)
- [License Requirements](#)
- [Port Requirements](#)
- [Web Browser Requirements](#)
- [Tenable Integrated Product Compatibility](#)

For detailed information about running Tenable.sc in a large enterprise deployments, see [Large Enterprise Deployments](#).



Hardware Requirements

You can run Tenable.sc 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.sc or Tenable Core + Tenable.sc in an environment shared with other Tenable applications.

Storage Requirements

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

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

Disk Space Requirements

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

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

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

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

Requirements When Running Basic Network Scans + Local Checks



Version	# of Hosts Managed by Tenable.sc	CPU Cores	Memory	Disk Space used for Vulnerability Trending
5.x	2,500 active IPs	4 2GHz cores	8 GB RAM	90 days: 125 GB 180 days: 250 GB
	10,000 active IPs	8 3GHz cores	16 GB RAM	90 days: 450 GB 180 days: 900 GB
	25,000 active IPs	16 3GHz cores	32 GB RAM	90 days: 1.2 TB 180 days: 2.4 TB
	100,000 active IPs	32 3GHz cores	64 GB RAM	90 days: 4.5 TB 180 days: 9 TB

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

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



Version	# of Hosts Managed by Tenable.sc	CPU Cores	Memory	Disk Space used for Vulnerability Trending
	IPs	cores		180 days: 18 TB

Disk Partition Requirements

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

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

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

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

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

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

Network Interface Requirements

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

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



Cloud Requirements

The primary method to deploy Tenable.sc in a cloud environment is with Tenable Core + Tenable.sc. For more information, see the [Tenable Core User Guide](#).

However, you can install Tenable.sc in vendor-supported version of your cloud environment that meets the [operating system requirements](#) to run Tenable.sc.

The following guidelines can help you install Tenable.sc in an Amazon Elastic Compute Cloud (Amazon EC2) cloud-based environment 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.

- [Supported Amazon EC2 Instance Types](#)
- [Supported Amazon Machine Images \(AMIs\)](#)
- [Supported Azure Instance Types](#)
- [Supported Azure Machine Images](#)

Supported Amazon EC2 Instance Types

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

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

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

Requirements When Running Basic Network Scans + Local Checks

# of Hosts Managed by Tenable.sc	EC2 Instance Type	Disk Space Used for Vulnerability Trending
1 to 2,500	m5.2xlarge	90 days: 125 GB



		180 days: 250 GB
2,501 to 10,000	m5.4xlarge	90 days: 450 GB 180 days: 900 GB
10,001 to 25,000	m5.8xlarge	90 days: 1.2 TB 180 days: 2.4 TB
25,001 to 50,000	m5.12xlarge	90 days: 4.5 TB 180 days: 9 TB
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.sc	EC2 Instance Type	Disk Space Used for Vulnerability Trending
1 to 2,500	m5.4xlarge	90 days: 225 GB 180 days: 450 GB
2,501 to 10,000	m5.8xlarge	90 days: 900 GB 180 days: 1.8 TB
10,001 to 25,000	m5.8xlarge	90 days: 2.25 TB 180 days: 4.5 TB
25,001 to 50,000	m5.12xlarge	90 days: 9 TB 180 days: 18 TB
50,001 or more	For assistance with large enterprise deployments greater than 50,000 active IP addresses, contact your Tenable representative.	

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.sc without Tenable Core:

AMI	Required Configuration Changes
CentOS 7 (x86_64) - with Updates HVM	- This AMI does not include Java, but Tenable.sc 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.sc. For more information, see Dependencies. - This AMI configures an SELinux enforcing mode policy, which requires customization to be compatible with Tenable.sc. You must use the SELinux <code>sealert</code> tool to identify errors and solutions. For more information, see Customize SELinux Enforcing Mode Policies for Tenable.sc. - You must confirm this AMI meets all other standard requirements for operating systems. For more information, see Operating System Requirements.

Supported Azure Instance Types

You can install Tenable.sc 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.sc 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.sc	Virtual Machine Instance	Disk Space Used for Vulnerability Trending
1 to 2,500	D3V2	90 days: 125 GB



		180 days: 250 GB
2,501 to 10,000	D4V2	90 days: 450 GB 180 days: 900 GB
10,001 to 25,000	F16	90 days: 1.2 TB 180 days: 2.4 TB
25,001 to 50,000	F32SV2	90 days: 4.5 TB 180 days: 9 TB
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.sc	EC2 Instance Type	Disk Space Used for Vulnerability Trending
1 to 2,500	D3V2	90 days: 225 GB 180 days: 450 GB
2,501 to 10,000	D4V2	90 days: 900 GB 180 days: 1.8 TB
10,001 to 25,000	F16	90 days: 2.25 TB 180 days: 4.5 TB
25,001 to 50,000	D32SV3	90 days: 9 TB 180 days: 18 TB
50,001 or more	For assistance with large enterprise deployments greater than 50,000 active IP addresses, contact your Tenable representative.	

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 image for Tenable.sc:

AMI	Required Configuration Changes
CIS CentOS Linux 7 Benchmark L1	• This image does not include Java, but Tenable.sc 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.sc. For more information, see Dependencies. • This image configures an SELinux enforcing mode policy, which requires customization to be compatible with Tenable.sc. You must use the SELinux <code>sealert</code> tool to identify errors and solutions. For more information, see Customize SELinux Enforcing Mode Policies for Tenable.sc. • You must confirm this image meets all other standard requirements for operating systems. For more information, see Operating System Requirements.



System Requirements

- [Operating System Requirements](#)
- [SELinux Requirements](#)
- [Secure Environment Requirements](#)
- [Dependencies](#)
- [Tenable.sc Communications and Directories](#)

Operating System Requirements

This version of Tenable.sc is available for:

- Red Hat Enterprise Linux 6 (RHEL 6), 64-bit
- Red Hat Enterprise Linux 7 (RHEL 7), 64-bit
- CentOS 6, 64-bit
- CentOS 7, 64-bit
- Red Hat Enterprise Linux 7 (RHEL 7), 64-bit
- Red Hat Enterprise Linux 8 (RHEL 8), 64-bit
- CentOS 7, 64-bit

SELinux Requirements

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

- Disabled and permissive mode policies typically do not require customization to interact with Tenable.sc.
- Enforcing mode policies require customization to interact with Tenable.sc. For more information, see [Customize SELinux Enforcing Mode Policies for Tenable.sc](#).

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



Secure Environment Requirements

Tenable recommends adhering to security best practices, including:

- Configure the operating system to ensure that security controls cannot be bypassed.
- Configure the network to ensure that the Tenable.sc system resides in a secure network segment that is not accessible from the Internet.
- Configure network time synchronization to ensure that accurate time stamps are recorded in reports and log files.

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

- Configure access control to ensure that only authorized users have access to the operating system platform.
- Monitor system resources to ensure that adequate disk space and memory are available, as described in [Hardware Requirements](#). If system resources are exhausted, Tenable.sc may not log audit data during system administrator troubleshooting or other activities. For more information about troubleshooting resource exhaustion, see [General Tenable.sc Troubleshooting](#).

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

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

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

Dependencies

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



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

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

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

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

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

- or -

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

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

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

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

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

Tenable.sc Communications and Directories

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

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



Tenable.sc 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.sc or for offline installation. Plugin packages are secured via 4096-bit RSA digital signatures. For more information, see Port Requirements.

For information about data encryption in Tenable.sc, see [Encryption Strength](#).



Customize SELinux Enforcing Mode Policies for Tenable.sc

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

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

Tenable.sc restarts.

4. Run the `sealert` tool again to confirm you resolved the error alerts.



Use /dev/random for Random Number Data Generation

Required User Role: Root user

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

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

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

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

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

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

```
export TSC_ENTROPY_CHECK=true
```

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

What to do next:

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



License Requirements

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

You can update your Tenable.sc license in an externally connected or air-gapped environment, as described in [Update an Existing License](#).

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

Tip: For information about Tenable.sc-Tenable product registration server communications encryption, see [Encryption Strength](#).

Your Tenable.sc License

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

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

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

Counted Toward License	Not Counted Toward License
- IP addresses from active scans - IP addresses from Log Correlation Engine instances - IP addresses from NNM instances not	- IP addresses present only from imports to offline repositories - IP addresses present only from NNM instances in discovery mode



Counted Toward License	Not Counted Toward License
in discovery mode UUIDs from Tenable.ot instances A single IP address or UUID counts once toward your license, even if it was scanned by multiple methods or stored in multiple repositories. Note: If you use an alternative port scanner, Tenable.sc counts the detected IP addresses against your license.	The following excluded plugins: Nessus — 10180, 10287, 10335, 11219, 11933, 11936, 12053, 14272, 14274, 19506, 22964, 33812, 33813, 34220, 34277, 45590, 54615, 87413, and 112154. NNM — 0, 12, 18, 19, 20, 113, and 132. LCE — 800000 through 800099.

Your Tenable.sc Continuous View Product Licenses

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

Your Lumin License

If you want to view and analyze your data in Tenable.io using Lumin, you must acquire a Tenable.io Lumin license for use with your Tenable.sc deployment.

Tip: Synchronized assets that count toward your Tenable.sc license also count toward your Tenable.io license.

For more information, contact your Tenable representative.



Apply a New License

Required User Role: Administrator

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

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

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

1. Log in to Tenable.sc via the user interface.
2. Click **System > Configuration**.

The **Configuration** page appears.

3. Click the **License** tile.

The **License Configuration** page appears.

4. Click the product box for the license you want to apply.
5. In the box, type the activation code for the product.
6. Click **Register**.

Tenable.sc updates the page to reflect the activation code status:

- Valid Code: A green box with a check mark.
- Invalid Code: A red box with an X.

If the code is valid, Tenable.sc initiates a plugin download.



Update an Existing License

Required User Role: Administrator

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

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

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

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

To update a license:

1. Log in to Tenable.sc via the user interface.
2. Click **System > Configuration**.

The **Configuration** page appears.

3. Click the **License** tile.

The **License Configuration** page appears.

4. To replace your Tenable.sc license, in the **Tenable.sc License** section:

- a. Click **Update License**.
- b. Click **Choose File** and browse to the license file you want to upload.

Tenable.sc applies the new license.

5. To replace an activation code for an integrated product license, in the **Additional Licenses** section:

- a. Click the green check mark.
- b. Click **Reset Activation Code**.
- c. In the box, paste your product license activation code.
- d. Click **Register**.



Tenable.sc communicates with the Tenable product registration server to validate your license activation code.

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



Tenable.sc CV License Expiration

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

Tenable.sc Console

- Perpetual license—The software remains fully functional. All user data is accessible. However, the Tenable.sc feed stops (that is, Tenable.sc no longer receives new plugin updates, dashboard updates, report updates, or audit file updates). Scan and data collection functionality is inhibited as described in the NNM, LCE, and Nessus sections below.
- Subscription license—You can no longer access the console unless you enter a new license key. Normal operation resumes once you replace the license key.

Nessus

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

NNM

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

LCE

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



Port Requirements

Your Tenable.sc deployment requires 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.sc.
TCP 443	Accessing the Tenable.sc user interface. Accessing the Tenable.sc API interface. Performing automatic SSH key setup to synchronize remote repositories with another Tenable.sc.

Outbound Traffic

You must allow outbound traffic to the following ports.

Port	Traffic
TCP 25	Sending SMTP email notifications.
TCP 443	Communicating with Tenable.io. Communicating with the <code>plugins.nessus.org</code> server for plugin updates.
TCP 1243	Communicating with Log Correlation Engine.
TCP 8834	Communicating with Nessus.
TCP 8835	Communicating with Nessus Network Monitor.
UDP 53	Performing DNS resolution.



Web Browser Requirements

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

- Microsoft Internet Explorer 11 or later
- Mozilla Firefox 32 or later
- Google Chrome 37 or later
- Mac OS Safari 7.1 or later



Tenable Integrated Product Compatibility

The release notes list the versions of Tenable products tested with Tenable.sc 5.16.x. For more information, see the [Tenable.sc Release Notes](#) for your version.



Large Enterprise Deployments

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



Installation and Upgrade

To perform a fresh installation of Tenable.sc, see [Before You Install](#) and [Install Tenable.sc](#).

To perform an upgrade of Tenable.sc, see [Before You Upgrade](#) and [Upgrade Tenable.sc](#).

To uninstall Tenable.sc, see [Uninstall Tenable.sc](#).



Before You Install

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

Understand Tenable.sc Licenses

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

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

Disable Default Web Servers

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

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

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

Modify Security Settings

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

Perform Log File Rotation

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

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

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



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

Allow Tenable Sites

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



Install Tenable.sc

Required User Role: Root user

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

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

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

For information about new features, resolved issues, third-party product updates, and supported upgrade paths, see the [release notes](#) for Tenable.sc 5.16.x.

Before you begin:

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

To install Tenable.sc:

1. On the host where you want to install Tenable.sc, open the command line interface (CLI).
2. Run one of the following commands to Install the RPM:

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

- or -



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

Output similar to the following is generated:

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

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

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



Quick Setup

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

- [License](#)
- [Nessus Scanner](#)
- [NNM](#)
- [LCE](#)
- [Repository](#)
- [Organization](#)
- [LDAP](#)
- [User](#)
- [Additional Settings](#)

After configuring, [Review](#) and confirm.

License

Upload your Tenable.sc license and apply additional product licenses.

Tenable.sc License

1. Click **Choose File** to upload the Tenable.sc 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.

Additional Licenses

Consider adding additional license activation codes:



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

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

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

In the **NNM** section, type the NNM activation code and click **Register**.

- LCE Activation Code — required before downloading LCE Event vulnerability plugins to Tenable.sc. The LCE Activation Code allows Tenable.sc to download event plugins, but it does not manage plugin updates for LCE servers.

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

Click **Next** to continue.

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

A box with a checkmark indicates a valid license is applied and that Tenable.sc initiated a plugin download in the background.

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

Nessus Scanner

Configure your first Nessus scanner. For information about the options you can configure, see [Nessus Scanners](#). There are some limitations on the scanner options you can configure during Quick Start:

- **Agent Capable:** If you use a Tenable.io or Nessus Manager scanner for Nessus Agent scan imports, do not configure that scanner during the Quick Start.
- **Zones:** If you want to grant scan zones access to this scanner, you must configure the **Zones** option after the Quick Start.

NNM



If you added an NNM license activation code, you can configure your first NNM scanner. For information about the options you can configure, see [Nessus Network Monitor Instances](#). There are some limitations on the scanner options you can configure during Quick Start:

- **Repositories:** If you want to select repositories to store the scanner's data, you must configure the **Repositories** option after the Quick Start.

LCE

If you added an LCE Activation Code, you can configure your first Log Correlation Engine scanner. For information about the options you can configure, see [Log Correlation Engines](#). There are some limitations on the scanner options you can configure during Quick Start:

- **Organizations:** If you want to select organizations that can access the scanner's data, you must configure the **Organizations** option after the Quick Start.
- **Repositories:** If you want to select repositories to store the scanner's data, you must configure the **Repositories** option after the Quick Start.

Repository

You can configure your first local IPv4 or IPv6 repository.

Caution: When creating repositories, note that IPv4 and IPv6 addresses must be stored separately. Additional repositories may be created once the initial configuration is complete.

A repository is essentially a database of vulnerability data defined by one or more ranges of IP addresses. When the repository is created, a selection for IPv4 or IPv6 addresses must be made. Only IP addresses of the designated type may be imported to the designated repository. The organization created in steps that follow can take advantage of one or more repositories. During installation, a single local repository is created with the ability to modify its configuration and add others post-install.

Caution: When creating Tenable.sc repositories, LCE event source IP address ranges must be included along with the vulnerability IP address ranges or the event data is not accessible from the Tenable.sc UI.

Local repositories are based on the IP addresses specified in the **IP Ranges** option on this page during the initial setup. *Remote* repositories use addressing information pulled over the network from a



remote Tenable.sc. Remote repositories are useful in multi-Tenable.sc configurations where security installations are separate but reports are shared. *Offline* repositories also contain addressing information from another Tenable.sc. However, the information is imported to the new installation via a configuration file and not via a direct network connection. For information about how this works in air-gapped environments, see [Considerations for Air-Gapped Environments](#).

For information about the options you can configure, see [Local Repositories](#). There are some limitations on the repositories and repository options you can configure during Quick Start:

- You cannot configure a local mobile repository during Quick Start.
- You cannot configure a local agent repository during Quick Start.
- You cannot configure an external repository during Quick Start.
- **Organizations:** If you want to select organizations that can access the repository's data, you must configure the **Organizations** option after the Quick Start.
- **LCE Correlation:** If you want to select LCE servers where you want Tenable.sc to retrieve data, you must configure the **LCE Correlation** option after the Quick Start.

Organization

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

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

LDAP

Configuring LDAP allows you to use external LDAP servers for the Tenable.sc user account authentication or as LDAP query assets. Type all required LDAP server settings and click **Next**. Click **Skip** if you do not want to configure LDAP during initial configuration.

You can configure one LDAP server connection during initial setup. If you want to use multiple LDAP servers, or if you want to configure additional options, you must continue configuring LDAP after the Quick Start.

For information about the options you can configure, see [LDAP Authentication](#).



User

You must create one administrator and one security manager during initial setup. For more information, see [User Roles](#).

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

If you already configured an LDAP server, you have the option to create an LDAP user account. For more information about user account options, see [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.

Additional Settings

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

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

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

For more information about enabling or disabling this option after initial setup, see [Configuration Settings](#).

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.

- [Tenable.sc Upgrade Path](#)
- [Java Version Requirements](#)
- [Halt or Complete Running Jobs](#)
- [Perform a Tenable.sc Backup](#)
- [Rename Your Mount Point](#)

Tenable.sc Upgrade Path

For more information about the upgrade paths to Tenable.sc version 5.16.x, see the [Tenable.sc Release Notes](#).

Java Version Requirements

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

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

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

Halt or Complete Running Jobs

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

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



Stop the processes manually or retry the upgrade after the processes complete.

Perform a Tenable.sc Backup

Perform a backup of Tenable.sc before beginning your upgrade. For more information, see [Backup and Restore](#).

Rename Your Mount Point

If the existing `/opt/sc` directory is or contains a mount point to another location, rename the mount point. During the RPM upgrade process, a message appears with information about the discovered mount point. Contact your system administrator for assistance.



Upgrade Tenable.sc

Required User Role: Root user

Note: This topic assumes a basic understanding of Linux.

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

For information about new features, resolved issues, third-party product updates, and supported upgrade paths, see the [release notes](#) for Tenable.sc 5.16.x.

Before you begin:

1. Complete system prerequisites, as described in [Before You Upgrade](#).

Note: Tenable recommends creating a backup of your Tenable.sc 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.sc to use `/dev/random` instead of `/dev/urandom` to generate random number data for secure communication functions, modify the random data source as described in [Use /dev/random for Random Number Data Generation](#).

To upgrade to Tenable.sc 5.16.x:

1. Log in to Tenable.sc via the user interface.
2. Pause all running scans, as described in [Start or Pause a Scan](#).
3. Prepare the upgrade command you intend to run:



- Use `rpm` with the “-Uvh” switches from the command-line of the Tenable.sc server.
- Use “`sudo -i`” when performing sudo upgrades of Tenable.sc to ensure the proper use of environmental variables.

For example:

```
# rpm -Uvh SecurityCenter-x.x.x-el6.x86_64.rpm
```

- or -

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

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

```
# rpm -Uvh SecurityCenter-x.x.x-el6.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:

- (Optional) If you used custom Apache SSL certificates before upgrading Tenable.sc, restore the custom SSL certificates, as described in [Restore Custom SSL Certificates](#).



Restore Custom SSL Certificates

Required User Role: Root user

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

Tenable.sc creates a backup of the certificates during the upgrade process. Tenable.sc 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.sc, as described in [Upgrade Tenable.sc](#).

To restore custom SSL certificates after upgrading Tenable.sc:

1. Log in to Tenable.sc via the command line interface (CLI).
2. In the CLI in Tenable.sc, 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.sc, 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.sc, 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.



Uninstall Tenable.sc

Required User Role: Root user

To uninstall Tenable.sc:

1. On the host where you want to uninstall Tenable.sc, open the command line interface (CLI).
2. In the CLI, run the following command to stop Tenable.sc:

```
service SecurityCenter stop
```

3. Run the following command to determine the name of the RPM package:

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

The name of the RPM package appears.

4. Run one of the following commands to remove the Tenable.sc:

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

- or -

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

5. Run the following command to remove user-created and user-modified files:

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

Tenable.sc is removed.



User Access

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

There are two categories of user accounts:

- *Administrator* users have the system-provided administrator role and do not belong to organizations.
- *Organizational* users have the system-provided security manager, auditor, credential manager, executive, security analyst, security manager, or vulnerability analyst role, or a custom role, and belong to an organization.

Tenable.sc supports three types of user account authentication: TNS, LDAP, and SAML. For more information, see [User Accounts](#).

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



Log In to the Web Interface

Required User Role: Any

To log in to the Tenable.sc configuration interface:

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

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

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

2. Clear your web browser's cache.
3. Navigate to the URL for your Tenable.sc: `https://<SERVER ADDRESS OR NAME>/`.

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

The Tenable.sc web interface appears.

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

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

- To log in via a username and password, type your Tenable.sc credentials and click **Log In**.
- To log in via SAML authentication, click **Sign In Using Identity Provider**. When presented with your identity provider login page, type your identity provider credentials.

For more information about SAML authentication, see [Configure SAML Authentication Manually via the User Interface](#).

- To log in via certificate, see [Log in to the Web Interface via SSL Client Certificate](#).

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



Initial Login Considerations

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

If you prefer to configure the system manually, click **Exit Quick Setup Guide**. For more information about getting started with Tenable.sc, see [Get Started With Tenable.sc](#).



Log in to the Web Interface via SSL Client Certificate

Required User Role: Any

Before you begin:

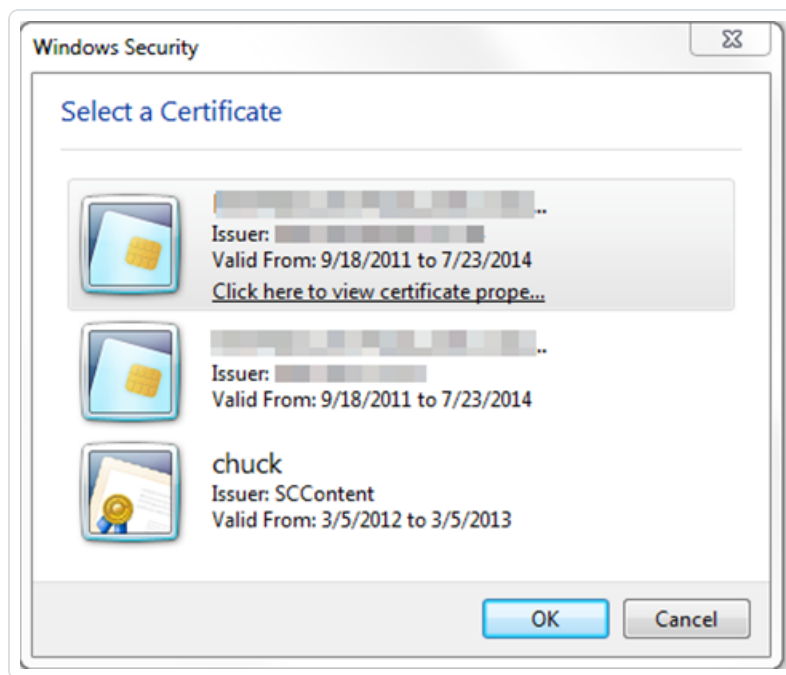
- Confirm your Tenable.sc administrator fully configured Tenable.sc for certificate authentication, as described in [Certificate Authentication](#).

To perform a certificate-based Tenable.sc login:

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

1. Open a browser window and navigate to Tenable.sc.

The browser presents a list of available certificate identities.



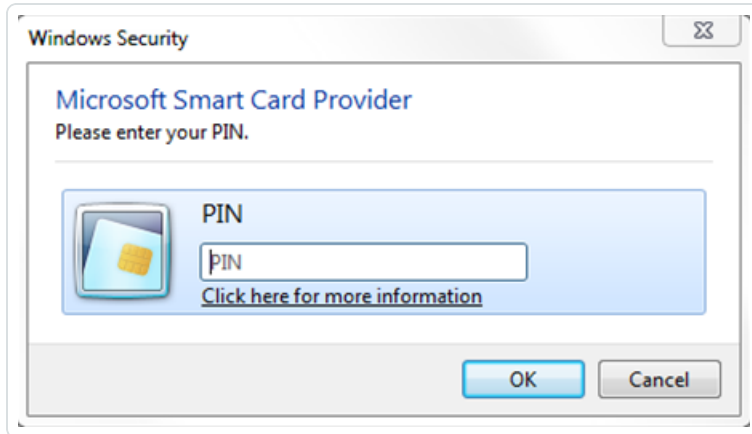
For information about Tenable.sc-browser communications encryption, see [Encryption Strength](#).

2. Select a certificate.



3. Click **OK**.

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



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

5. Click **OK**.

The Tenable.sc login page appears.

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

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

The **Certificate Authentication** window appears.

7. When prompted, specify whether the current certificate is to be used to authenticate the current user.
 - Click **Yes** to always use the certificate for authentication.
 - Click **No** to ignore the certificate and log in via TNS authentication.

Tenable.sc logs you in.

Subsequent Logins

After you log out of Tenable.sc, Tenable.sc displays the login page. If you want to log in again with the same certificate, refresh your browser window. If you want to use a different certificate, you must start a new browser session.



After you perform your second certificate login, edit your account from the **Profile** page to view your certificate details. If your certificate changes or you need to revoke it, click the **Clear Certification Details** button to disassociate the certificate from your account.



User Roles

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

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

For more information about user roles in Tenable.sc, see [Create a User Role](#), [Edit a User Role](#), [View User Role Details](#), and [Delete a User Role](#).

Roles

User Role	Customizable Permissions?	Description
Administrator	No	An account that manages Tenable.sc as a whole. The primary task of the Administrator is to install and configure each organization. In addition, the Administrator adds components to Tenable.sc such as NNM, LCE, and Nessus to extend its capabilities. The Administrator is automatically assigned the “Manage Application” role. Because administrators do not belong to an organization, they do not have access to the data collected by Tenable.sc.
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 have the ability to launch scans, configure users (except for administrator user roles), vulnerability



		policies, and other objects belonging to their organization. A Security Manager is the account within an organization that has a broad range of security roles within the defined organization. This is the initial user that is created when a new organization is created and has the ability to launch scans, configure users (except for the Administrator user), vulnerability policies, and other objects that belong to their organization. This initial Security Manager account cannot be deleted without deleting the entire organization. Security Managers have complete access to all data collected by their organization.
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 blackout 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
Scan 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 Agent Synchronization Jobs		Allows the user to add agent synchronization jobs that fetch agent scan results from Tenable.io or Nessus Manager.
Create Agent Scans		Allows the user to add agent scans that create and launch parallel scans in Nessus Manager, then import the scan results to Tenable.sc.



Permissions Option	Description
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.
Manage Blackout Windows	Allows the user to add, edit, and delete organization-wide blackout windows. Blackout 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.
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 will be able to use them 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, which can be used in reports by anyone in the organization.
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.sc 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.



Create a User Role

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

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

To create a custom user role:

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

2. 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 **Scanning Permissions**, **Asset Permissions**, **Analysis Permissions**, **Organization Permissions**, **User Permissions**, **Reporting Permissions**, **System Permissions**, and **Workflow Permissions**.

7. Click **Submit**.

Tenable.sc saves your configuration.



Edit a User Role

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

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

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

1. Log in to Tenable.sc via the user interface.
2. Click **Users > Roles**.

The **Roles** page appears.

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

The actions menu appears.

4. Click **Edit**.

The **Edit Role** page appears.

5. (Optional) Modify the **Name**
6. (Optional) Modify the **Description**.
7. (Optional) Modify the following permissions, as described in [User Roles](#)
 - **Scanning Permissions**
 - **Asset Permissions**
 - **Analysis Permissions**
 - **Organization Permissions**
 - **User Permissions**
 - **Reporting Permissions**
 - **System Permissions**
 - **Workflow Permissions**



8. Click **Submit**.

Tenable.sc saves your configuration.



View User Role Details

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

You can view details for any user role. For more information, see [User Roles](#).

To view role details:

1. Log in to Tenable.sc via the user interface.
2. Click **Users > Roles**.

The **Roles** page appears.

3. In the row for the user role, click the  menu.

The actions menu appears.

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 Per- missions	View a summary of permissions for the role. For more information, see User Roles.
Asset Permissions	



Section	Action
Analysis Per- missions	
Organization Per- missions	
User Permissions	
Reporting Per- missions	
System Per- missions	
Workflow Per- missions	



Delete a User Role

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

For more information, see [User Roles](#).

To delete a custom or system-provided user role:

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

1. Log in to Tenable.sc via the user interface.
2. Click **Users > Roles**.
The **Roles** page appears.
3. In the row for the role you want to delete, click the  menu.

The actions menu appears.

4. Click **Delete**.

A confirmation window appears.

5. Click **Delete**.

Tenable.sc deletes the role.



Organizations and Groups

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

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



Organizations

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

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

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

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

To view details for any organization, see [View Organization Details](#).

Organization Options

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.
Scanning	
Distribution Method	The scan distribution mode you want to use for this organization: • Automatic Distribution Only: Tenable.sc chooses one or



Option	Description
	more scan zones to run the scan. Organizational users cannot choose a scan zone when configuring a scan. Tenable.sc distributes targets for scans based on your configured scan zone ranges. This facilitates optimal scanning and is very 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.sc 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.sc 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. For more information about scan zones, see Scan Zones.
Available Zones	One or more scan zones that you want organizational users to have access to when configuring scans.
Allow for Automatic Distribution	Enable or disable this option to specify whether you want Tenable.sc to automatically select one or more scan zones if an organizational user does not specify a scan zone when configuring a scan. • When enabled, Tenable.sc chooses one or more scan zones as specified by your Restrict to Selected Zones setting. • When disabled, Tenable.sc requires the organizational user



Option	Description
	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.sc to choose from when automatically distributing zones. • When enabled, Tenable.sc chooses from the Available Zones shared with the organization. • When disabled, Tenable.sc chooses from all zones on Tenable.sc.
Restricted Scan Ranges	The IP address ranges you do not want users in this organization to scan.
Analysis	
Accessible LCEs	The LCEs that you want this organization to have access to. You can search for the LCEs by name or scroll through the list.
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 Nessus scanners (with Nessus Agents enabled) that you want this organization to have access to. Select one or more of the available scanners to allow the organization to import Nessus Agent results from the selected scanner.
Accessible LDAP Servers	The LDAP servers that you want this organization to have access to. An organization must have access to an LDAP server in order to perform LDAP authentication on user accounts within that organization, and to configure LDAP query assets. Note: If you revoke access to an LDAP server, users in the organization cannot authenticate and LDAP query assets cannot run.



Option	Description
Custom Analysis Links	
A list of custom analysis links provided to users within the host vulnerability details when analyzing data outside of Tenable.sc is desired. Click Add Custom Link to create a new option to type the link name and URL to look up additional data external to Tenable.sc. For example: <i>http://example.com/index.htm?ip=%ip%</i> The <i>%ip%</i> 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)



Add an Organization

Required User Role: Administrator

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

To add an organization:

1. Log in to Tenable.sc via the user interface.
2. Click **Organizations**.

The **Organizations** page appears.

3. Click **Add**.

The **Add Organization** page appears.

4. Configure the following settings:

- **General**
- **Scanning**
- **Analysis**
- **Custom Analysis Links**
- **Vulnerability Weights**

5. Click **Submit**.

Tenable.sc saves your configuration.



View Organization Details

Required User Role: Administrator

You can view details for any organization. For more information, see [Organizations](#).

To view organization details:

1. Log in to Tenable.sc via the user interface.
2. Click **Organizations**.

The **Organizations** page appears.

3. In the row for the organization, click the  menu.

The actions menu appears.

4. Click **View**.

The **View Organization** page appears.

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.
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



Section	Action
	more information about a setting, see Organizations .
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 .



Delete an Organization

Required User Role: Administrator

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

To delete an organization:

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

1. Log in to Tenable.sc via the user interface.
2. Click **Organizations**.
The **Organizations** page appears.
3. In the row for the organization you want to delete, click the  menu.

The actions menu appears.

4. Click **Delete**.

A confirmation window appears.

5. Click **Delete**.

Tenable.sc deletes the organization.



Groups

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

For more information, see [Add a Group](#), [View Group Details](#), and [Delete a Group](#).

Group Options

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 IP addresses and agent IDs that are viewable by the group. The selection is made by all defined assets or the selection of one or more asset lists.
Repositories	The repositories you want to share with the group.
LCEs	The LCEs you want to assign to 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) • sample ARCs (CCC 1: Maintain an Inventory of Software and Hardware, CCC 2: Remove Vulnerabilities and Misconfigurations, CCC 3:



Option	Description
	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.sc: - Assigns their dashboards and ARCs to a new sample content object owner in group A. Tenable.sc does not reassign reports or assets. - Recreates their dashboards, ARCs, and assets required for ARCs in group B. Tenable.sc 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.



Add a Group

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

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

To add a group:

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

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.sc saves your configuration.



View Group Details

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

You can view details for any group. For more information, see [Groups](#).

To view group details:

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

The **Groups** page appears.

3. In the row for the group, click the  menu.

The actions menu appears.

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 , Repositories , and LCEs users in the group can access. For more information, see Group Options .
Preferences	View whether you enabled Sample Content for the group. For more information, see Group Options .
Users	View the list of users associated with the group.



Delete a Group

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

To delete a group:

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

The **Groups** page appears.

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

The actions menu appears.

4. Click **Delete**.

A confirmation window appears.

5. Click **Delete**.

Tenable.sc deletes the group.



User Accounts

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

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

Linked User Accounts

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

API Keys

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

User Account Options

Option	Authentication Type	Description
Role	All	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:



Option	Authentication Type	Description
		• 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	All	The organization where you want to assign the user account.
First Name / Last Name	All	(Optional) The given first name and last name for the user.
Type	All	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 see LDAP or SAML in the Type drop-down box.
Username / Password	TNS	The username and password for the user account. When selecting a username, it is sometimes easier to focus on the person's real name as a convention (e.g., Bob Smith would become <i>bsmith</i>). However, it may also be useful to assign names based on role, such as <i>auditNY</i>. Note: The username value is case-sensitive.



Option	Authentication Type	Description
		Tip: Tenable recommends using passwords that meet stringent length and complexity requirements. For information about Tenable.sc password data encryption, see Encryption Strength.
Username	SAML	The user's SAML username. Type the username exactly as it appears in your identity provider SAML configuration for this user.
User Must Change Password	TNS	(Optional) When enabled, the user must change their password upon initial login.
LDAP Server	LDAP	The server you want to use to authenticate the user.
Search String	LDAP	The LDAP search string you want to use to filter your user search. Use the format: <i>attribute=<filter text></i>. You can use wildcards, and the option accepts up to 1024 characters. Examples sAMAccountName=* mail=a* displayName=C*
LDAP Users Found	LDAP	A filtered list of LDAP user accounts retrieved by the Search String . Your selection in this option populates the Username option.
Username	LDAP	(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.



Option	Authentication Type	Description
Time Zone	All	(Required) The time zone for the user.
Scan Result Default Time-frame	All	The default Completion Time filter applied when the user accesses or refreshes the scan results page.
Cached Fetching	All	(Optional) When enabled, Tenable.sc caches plugin policy information and performs plugin policy downloads once per page load.
Group	All	The group where you want to assign the user account. A user's group determines their access to Tenable.sc resources. For more information about groups, see Groups. To grant a user limited privileges to other groups' resources, see Custom Group Permissions.
Asset	All	(Optional) Assigns a user to an asset list for which the user is responsible. Assigning a user to an asset list makes it easier to determine who in a group or organization should be assigned tickets, notifications, and other tasks to resolve particular issues. Selecting an asset updates the User Responsibility Summary in the Vulnerability Analysis section.
Contact Information	All	(Optional) The contact information for the user.



Add a TNS-Authenticated User

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

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

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

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

2. Click **Users > Users**.

The **Users** page appears.

3. Click **Add**.

The **Add User** page appears.

4. Select a **Role**.

5. If you selected **Security Manager** as the **Role**, select an **Organization**.

6. (Optional) Type a **First Name** and **Last Name**.

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

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

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

10. Select a **Time Zone**.

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

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

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

14. Click **Submit**.

Tenable.sc saves your configuration.

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



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

The **Users** page appears.
3. Click **Add**.

The **Add User** page appears.
4. (Optional) Type a **First Name** and **Last Name** for the user.
5. If the **Type** drop-down box is visible, select **TNS**.
6. Type a **Username** and **Password** for the user.
7. (Optional) Enable **User Must Change Password**.
8. Select a **Time Zone**.
9. (Optional) Select a **Scan Result Default Timeframe**.
10. (Optional) Enable **Cached Fetching**.
11. Select a **Role**. For more information, see [User Roles](#).
12. Select a **Group**. For more information, see [Organizations and Groups](#).
13. (Optional) If you want to customize the group-related permissions for the user, modify the **Group Permissions** as described in [Custom Group Permissions](#).
14. (Optional) If you want to share an asset list with the user, select an **Asset**. For more information, see [Assets](#).
15. (Optional) Type **Contact Information** for the user.
16. Click **Submit**.

Tenable.sc saves your configuration.



Add an LDAP-Authenticated User

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

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

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

1. Log in to Tenable.sc via the user interface.
2. Configure an LDAP server, as described in [LDAP Authentication](#). If you want the new user to be a member of an organization, associate the LDAP server with an organization.
3. Click **Users > Users**.

The **Users** page appears.

4. Click **Add**.

The **Add User** page appears.

5. Select a **Role** for the user account.
6. If you selected **Security Manager** as the **Role**, select an **Organization** for the user account. You must select an organization with an associated LDAP server.
7. (Optional) Type a **First Name** and **Last Name** for the user.
8. In the **Type** drop-down list, select **LDAP**. If **LDAP** does not appear in the drop-down list, add an LDAP server as described in [Add an LDAP Server](#).

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

10. Type a **Search String** to find existing users on the LDAP server.

11. Click **Search**.

The page displays the **LDAP Users Found** by the LDAP search string.

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

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



13. View the **Username**. Tenable does not recommend modifying the **Username** since it must match the username on the LDAP server.
14. Select a **Time Zone**.
15. (Optional) Select a **Scan Result Default Timeframe**.
16. (Optional) Enable **Cached Fetching**.
17. (Optional) Type **Contact Information** for the user.
18. Click **Submit**.

Tenable.sc saves your configuration.

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

1. Log in to Tenable.sc via the user interface. You must log in with a user account belonging to the organization where you want to create a new user.
2. Confirm that an administrator user configured an LDAP server, and that the LDAP server was associated with the organization where you want to create a user account.
3. Click **Users > Users**.

The **Users** page appears.

4. Click **Add**.

The **Add User** page appears.

5. (Optional) Type a **First Name** and **Last Name** for the user.
6. In the **Type** drop-down list, select **LDAP**. If **LDAP** does not appear in the drop-down list, add an LDAP server as described in [Add an LDAP Server](#).
7. Select the **LDAP Server** where you want to authenticate the user.
8. Select an LDAP user from the **LDAP Users Found** drop-down box.

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

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



10. Select a **Time Zone**.
11. (Optional) Select a **Scan Result Default Timeframe**.
12. (Optional) Enable **Cached Fetching**.
13. Select a **Role**. For more information, see [User Roles](#).
14. Select a **Group**. For more information, see [Organizations and Groups](#).
15. (Optional) If you want to customize the group-related permissions for the user, modify the **Group Permissions** as described in [Custom Group Permissions](#).
16. (Optional) If you want to share an asset list with the user, select an **Asset**. For more information, see [Assets](#).
17. (Optional) Type **Contact Information** for the user.
18. Click **Submit**.

Tenable.sc saves your configuration.



Add a SAML-Authenticated User

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

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

Before you begin:

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

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

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



11. Click **Submit**.

Tenable.sc saves your configuration.

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

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

2. Click **Users > Users**.

The **Users** page appears.

3. Click **Add**.

The **Add User** page appears.

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

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

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

7. Select a **Time Zone**.

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

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

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

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

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

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

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



15. Click **Submit**.

Tenable.sc saves your configuration.



Manage User Accounts

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

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

To view or edit a user account:

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **Users > Users**.

The **Users** page appears.

3. To filter the users that appear on the page, apply a filter as described in [Apply a Filter](#).
4. To view details for a user, see [View User Details](#).

5. To edit a user:

- a. In the row for the user, click the  menu.

The actions menu appears.

- b. Click **Edit**.

The **Edit User** page appears.

- c. Modify the user details.

Note: If you want to edit a Tenable.sc user that was created via user provisioning and you enabled **User Data Sync**, edit the user in your SAML identity provider. Otherwise, the Tenable.sc user data synchronization overwrites your changes the next time the user logs in to Tenable.sc using your SAML identity provider. For more information about **User Data Sync**, see [SAML Authentication Options](#).

- d. Click **Submit**.

Tenable.sc saves your configuration.

6. To delete a user, see [Delete a User](#).



Edit Your User Account

Required User Role: Any

You can edit your user account to update your password, contact information, and other settings depending on your user role.

To edit your user account as an administrator:

1. Log in to Tenable.sc via the user interface.
2. Click **Users > Users**.

The **Users** page appears.

3. Click the row for your user account.

The **Edit User** page appears.

4. Modify your user account settings. For more information, see [User Accounts](#).
5. Click **Submit**.

Tenable.sc saves your configuration.

To edit your user account as an organizational user:

1. Log in to Tenable.sc 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 Accounts](#).
4. Click **Submit**.

Tenable.sc saves your configuration.



View User Details

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

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

To view details for a user:

1. Log in to Tenable.sc via the user interface.
2. Click **Users > Users**.

The **Users** page appears.

3. In the row for the user, click the  menu.
4. Click **View**.

The **View User** page appears.

5. View the following information for the user:

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 Accounts.
Contact Information	View contact information for the user. For more information, see User Accounts.
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 User Role: Administrator

View linked user accounts associated with the user:

- **Linked Users** – If the user is an Administrator, view the linked Security Manager users.
- **Primary User** – If the user is a Security Manager, view the linked Administrator user.

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



Delete a User

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

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

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

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

Note: If you want to delete a Tenable.sc user that was created via user provisioning, delete the user from your SAML identity provider. If you delete a user in Tenable.sc that was created via user provisioning without deleting the user in your SAML identity provider, Tenable.sc automatically re-creates the user in Tenable.sc the next time they log in using your SAML identity provider. For more information, see [SAML User Provisioning](#).

To delete a user:

1. Log in to Tenable.sc via the user interface.
2. Click **Users > Users**.

The **Users** page appears.

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

The actions menu appears.

4. Click **Delete**.

A confirmation window appears.

5. (Optional) If you want to migrate the user's objects, click the toggle to migrate the user's objects to another user. Tenable.sc supports migrating:
 - Active scans, agent scans, and scan results
 - Custom assets, credentials, audit files, and scan policies



- Blackout windows
- Queries
- Tickets and alerts
- ARCs
- Dashboards
- Reports, report images, report attributes, and report results

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

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

6. Click **Delete**.

Tenable.sc deletes the user.



Linked User Accounts

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

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

The following restrictions apply to linked user accounts:

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

For more information about user accounts in Tenable.sc, see [User Access](#) and [User Roles](#).

For more information about linked user accounts, see:

- [Add a Linked User](#)
- [Switch to a Linked User Account](#)
- [Delete a Linked User Account](#)



Add a Linked User

Required User Role: Administrator

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

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

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

To add a linked Security Manager to an Administrator:

1. Log in to Tenable.sc via the user interface.
2. Click **Users > Users**.

The **Users** page appears.

3. In the row for the Administrator for which you want to add a linked user, click the  menu.

The actions menu appears.

4. Click **Add Linked User**.

The **Add User** page appears. Tenable.sc pre-populates the **First Name**, **Last Name**, and **Contact Information** fields with values from the administrator user account.

5. Select an **Organization**.
6. (Optional) Modify the **First Name** and **Last Name** for the user.
7. Type a **Username** for the user.
8. Select a **Time Zone**.
9. (Optional) Select a **Scan Result Default Timeframe**.



10. (Optional) Enable **Cached Fetching**.
11. (Optional) Modify the **Contact Information** for the user.
12. Click **Submit**.

Tenable.sc saves your configuration.

What to do next:

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



Switch to a Linked User Account

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

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

Before you begin:

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

To switch to a linked user account:

1. Log in to Tenable.sc via the user interface.
2. **Note:** You must log into the Administrator user associated to the linked Security Manager, then switch between linked users. Linked Security Managers cannot log in to Tenable.sc directly.
3. Click **Username > Switch User**.

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

4. Click the name of the linked user you want to switch to.
5. Click **Switch**.

Tenable.sc logs you in as the selected user.

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



Edit a Linked User Account

Required User Role: Administrator or a Security Manager linked to an Administrator. For more information, see [User Roles](#) and [Linked User Accounts](#).

You can edit a linked user account as an administrator or while logged in as the linked user. For more information, see [Linked User Accounts](#).

To edit a linked user account as an administrator:

1. Log in to Tenable.sc via the user interface.
2. Click **Users > 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. Click the row for the linked user account you want to edit.

The **Edit User** page appears.

5. Modify the user account settings. For more information, see [User Accounts](#).
6. Click **Submit**.

Tenable.sc saves your configuration.

To edit your linked user account as a linked user:

1. Log in to Tenable.sc 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 Accounts](#).
5. Click **Submit**.

Tenable.sc saves your configuration.



Delete a Linked User Account

Required User Role: Administrator

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

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

To delete a linked user account:

1. Log in to Tenable.sc via the user interface.
2. Click **Users > Users**.

The **Users** page appears.

3. Apply a filter to view the organization for the user you want to delete, as described in [Apply a Filter](#).
4. In the row for the user you want to delete, click the  menu.

The actions menu appears.

5. Click **Delete**.

A confirmation window appears.

6. (Optional) If you want to migrate the user's objects, click the toggle to migrate the user's objects to another user. Tenable.sc supports migrating:
 - Active scans, agent scans, and scan results
 - Custom assets, credentials, audit files, and scan policies
 - Blackout windows
 - Queries
 - Tickets and alerts



- ARCs
- Dashboards
- Reports, report images, report attributes, and report results

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

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

7. Click **Delete**.

Tenable.sc 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) 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 (launch, import, copy, send to report, stop, pause, and delete) • Policies (edit, copy, and delete) • Assets (edit, share, and delete) • Alerts (edit and delete)



Resources Controlled by Manage Users/User Permissions	Resources Controlled by Manage Objects/Object Permissions
	• Audit files (edit, share, and delete) • Credentials (edit, share, and delete) • Tickets (edit, resolve, and close) • Risk rules (delete) • Queries (edit, share, and delete) • ARCs (edit, share, copy, and delete) • Dashboards (edit, share, copy, and delete)

Examples

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

Control Permissions to Resources in the User's Assigned Group

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

Control Permissions to Resources in Other Groups

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

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



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



Generate API Keys

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

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

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

Before you begin:

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

To generate API keys:

1. Log in to Tenable.sc via the user interface.
2. Click **Users > Users**.

The **Users** page appears.

3. In the row for the user for which you want to generate an API key, click the  menu.

The actions menu appears.

4. Click **Generate API Key**.

A confirmation window appears.

5. Click **Generate**.

The **Your API Key** window appears, displaying the access key and secret key for the user.

6. Save the API keys in a safe location.

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



What to do next:

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



Delete API Keys

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

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

To delete API keys:

1. Log in to Tenable.sc via the user interface.
2. Click **Users > Users**.

The **Users** page appears.

3. In the row for the user for which you want to delete API keys, click the  menu.

The actions menu appears.

4. Click **Delete API Key**.

A confirmation window appears.

5. Click **Delete**.

The system deletes the API keys.



LDAP Authentication

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

After you configure an LDAP server, create Tenable.sc user accounts for each LDAP user you want to grant access. For more information, see [Add an LDAP-Authenticated User](#).

You can also use configured LDAP servers as LDAP query assets. For more information, see [Assets](#).

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

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

For more information, see [Add an LDAP Server](#) and [Delete an LDAP Server](#).

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.



Option	Description
Encryption	If the LDAP server encrypts communications, the encryption method: Transport Layer Security (STARTTLS) or LDAP over SSL (LDAPS).
Username / Password	If required by the server, 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. Format the username as provided by the LDAP server. Tip: It is recommended to use passwords that meet stringent length and complexity requirements.
LDAP Schema Settings	
Base DN	(Required) The LDAP search base used as the starting point to search for the user data.
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.



Option	Description
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.sc organizations you want to authenticate using this LDAP server.
Advanced Settings	
Lowercase	When enabled, Tenable.sc 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.sc.
Time Limit	The number of seconds you want Tenable.sc to wait for search results from the LDAP server. Tenable recommends using the default value provided by Tenable.sc.

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



Add an LDAP Server

Required User Role: Administrator

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

To add an LDAP server connection:

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

What to do next:

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



Delete an LDAP Server

Required User Role: Administrator

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

To delete an LDAP server connection:

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

1. Log in to Tenable.sc via the user interface.
2. Click **Resources > LDAP Servers**.
3. In the row for the server connection you want to delete, click the  menu.

The actions menu appears.

4. Click **Delete**.

A confirmation window appears.

5. Click **Delete**.

Tenable.sc deletes the LDAP server.



LDAP Servers with Multiple OUs

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

For general information about LDAP Servers, see [LDAP Authentication](#).

Option 1 (Recommended)

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

Before you begin:

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

To configure LDAP with multiple OUs (Option 1):

1. Log in to Tenable.sc via the user interface.
2. Click **Resources > LDAP Servers**.
3. Add the LDAP server, as described in [Add an LDAP Server](#).

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

4. Log out of Tenable.sc.
5. Log in to Tenable.sc 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.sc via the user interface.
2. Click **Resources > LDAP Servers**.
3. Begin configuring the LDAP server, as described in [Add an LDAP Server](#).



LDAP Configuration

← Back

Test LDAP Settings

Server Settings

Hostname192.168.55.33

Port636

EncryptionLDAPS

UsernameTARGET\Administrator

PasswordPassword Set

LDAP Schema

Base DNDC=target.DC=example.DC=com

User Object FiltermemberOf=CN=nested1,OU=cftest1,DC=t

User Schema Settings

Username AttributesAMAccountName

E-mail Attributemail

Phone AttributetelephoneNumber

Name AttributeCN

Submit

Cancel

- Click **Test LDAP Settings** to test configurations.
- Log out of Tenable.sc.
- Log in to Tenable.sc as the organizational user you want to manage the users.
- 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.sc users can use identity provider-initiated single sign-on (SSO) when logging in to Tenable.sc. Tenable.sc supports:

- SAML 2.0-based authentication (e.g., Okta, OneLogin, Microsoft ADFS, etc.)
- Shibboleth 1.32.0 authentication

For more information, see:

- [Configure SAML Authentication Automatically via the User Interface](#)
- [Configure SAML Authentication Manually via the User Interface](#)
- [Configure SAML Authentication via the SimpleSAML Module](#)

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

- To manually add SAML-authenticated users in Tenable.sc, 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.sc using the **Sign In Using Identity Provider** button, as described in [Log In to the Web Interface](#).

Considerations for Advanced SAML Features

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

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

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.sc.
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, OneLogin, etc.) or Shibboleth 1.32.0.
Entity ID	The name of the Entity ID attribute. Type the attribute exactly as it appears in your identity provider SAML configuration. 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.sc to recognize users who match the format NameID=user-



Option	Description
	<i>name.</i>
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 <code>===BEGIN CERT===</code> and the <code>===END CERT===</code> strings.
User Provisioning	You can enable user provisioning to automatically create SAML-authenticated users in Tenable.sc by importing user accounts from your SAML identity provider. When user provisioning is enabled, users who log into your SAML identity provider are automatically created in Tenable.sc. For more information, see SAML User Provisioning. Note: If you want to delete a Tenable.sc user that was created via SAML user provisioning, delete the user from your SAML identity provider. If you delete a user in Tenable.sc that was created via SAML user provisioning without deleting the user in your SAML identity provider, Tenable.sc automatically re-creates the user in Tenable.sc 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.sc to automatically synchronize contact information from your SAML identity provider for Tenable.sc users created via SAML user provisioning. For more information, see SAML User Provisioning. Note: If you want to edit a Tenable.sc 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.sc user data sync overwrites your changes the next time the user logs in to Tenable.sc using your SAML identity provider. Note: Tenable.sc does not update required fields (Organization ID, Group ID, and Role ID). To change the organization, group, or role for a user created via SAML user provisioning, see Manage User Accounts.



Configure SAML Authentication Automatically via the User Interface

Required User Role: Administrator

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

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

Before you begin:

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

To automatically configure SAML authentication for Tenable.sc users:

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **System > Configuration**.

The **Configuration** page appears.

3. Click the **SAML** button.

The **SAML Configuration** page appears.

4. In the **General** section, confirm the **SAML** toggle is enabled.

If you want to disable SAML authentication for Tenable.sc users, click the toggle.

5. In the **Source** drop-down box, select **Import**.

The page updates to display additional options.

6. In the **Type** drop-down box, select **SAML 2.0** (e.g., Okta, OneLogin, etc.) or **Shibboleth 1.32.0**.
7. Click **Choose File** and browse to the SAML metadata file from your identity provider.

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



8. Click **Submit**.

Tenable.sc saves your configuration.

What to do next:

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



Configure SAML Authentication Manually via the User Interface

Required User Role: Administrator

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

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

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

Before you begin:

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

To configure SAML authentication for Tenable.sc users:

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **System > Configuration**.

The **Configuration** page appears.

3. Click the **SAML** button.

The **SAML Configuration** page appears.

4. In the **General** section, confirm the **SAML** toggle is enabled.

If you want to disable SAML authentication for Tenable.sc users, click the toggle.

5. In the **Source** drop-down box, select **Entry**.

The page updates to display additional options.



6. In the **SAML Settings** section, configure the options:
 - a. In the **Type** drop-down box, select **SAML 2.0** (e.g., Okta, OneLogin, etc.) or **Shibboleth1.32.0**.
 - b. In the **Entity ID** box, type the name of the Entity ID attribute exactly as it appears in your identity provider SAML configuration.
 - c. In the **Identity Provider (IdP)** box, type identity provider identifier string.
 - d. In the **Username Attribute** box, type the SAML username attribute exactly as it appears in your identity provider SAML configuration.
 - e. In the **Single Sign-on Service** box, type the identity provider URL where users log in via single sign-on exactly as it appears in your identity provider SAML metadata.
 - f. In the **Single Logout Service** box, type the identity provider URL where users log out exactly as it appears in your identity provider SAML metadata.
 - g. In the **Certificate Data** box, paste the text of the identity provider's X.509 SSL certificate, without the `===BEGIN CERT===` and the `===END CERT===` strings.
7. Click **Submit**.

Tenable.sc saves your configuration.

What to do next:

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



Configure SAML Authentication via the SimpleSAML Module

Required User Role: Administrator

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

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

Before you begin:

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

To configure SAML authentication via the SimpleSAML module:

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **System > Configuration**.

The **Configuration** page appears.

3. Click the **SAML** button.

The **SAML Configuration** page appears.

4. Type placeholder values into all SAML configuration options. You do not need to configure valid values.
5. Click **Submit**.

Tenable.sc saves your configuration.

6. Log in to Tenable.sc via the command line interface (CLI).
7. Navigate to and open the `/opt/sc/src/lib/SimpleSAML/config/authsources.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. In a browser, navigate to **`https://<Tenable.sc IP address or hostname>/sam-
I/module.php/core/frontpage_config.php`**.

The **SimpleSAML.php installation** page appears.
11. On the **Configuration** tab, click **Login as administrator**.

The **Enter your username and password** page appears.
12. In the **Username** box, type *admin*.
13. In the **Password** box, type *admin*.
14. Click **Login**.
15. On the **Federation** tab, in the **Tools** section, click **XML to SimpleSAML.php metadata con-
verter**.

The **Metadata parser** page appears.
16. Click **Choose File** and select your identity provider SAML metadata file.
17. Click **Parse**.

Tenable.sc validates the identity provider SAML metadata file. If the metadata file is sup-
ported, Tenable.sc populates the XML metadata box with content from your metadata file. If
the metadata file is not supported, you cannot use it for SAML authentication in Tenable.sc.
18. In the **saml20-idp-remote** section, copy the text in the box.
19. Log in to Tenable.sc via the command line interface (CLI).
20. Navigate to and open the `/opt/sc/src/lib/SimpleSAML/metadata/saml20-idp-
remote.php` file (for SAML 2.0) or `/opt/sc/src/lib/SimpleSAML/metadata/shib13-idp-
remote.php` file (for Shibboleth 1.32.0).



21. Paste the text into the file, after the `<?php` line.
22. Save the file.
23. Navigate to and open the `/opt/sc/src/lib/SimpleSAML/config/authsources.php` file again.
24. Confirm the **idp** URL in the `authsources.php` file matches the **\$metadata** URL in the `saml20-idp-remote.php` or `shib13-idp-remote.php` file:

Valid `authsources.php` syntax example:

```
'idp' => 'http://www.okta.com/abcdefghijklmnopQr0s1'
```

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

```
$metadata['http://www.okta.com/abcdefghijklmnopQr0s1']
```

25. In a browser, navigate to **`https://<Tenable.sc IP address or hostname>/saml/module.php/core/frontpage_config.php`**.

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

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

The **Test authentication sources** page appears.

27. Click **1**.

Your identity provider login page appears.

28. Log in to your identity provider.

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

What to do next:

- In the Tenable.sc interface, on the **SAML Configuration** page, click **Download SAML Configuration XML**, save the `.xml` file locally, and use it to configure your identity provider SAML configuration. For more information, see [SAML Authentication XML Configuration](#)



Examples.

- Add SAML-authenticated user accounts.
 - To manually add SAML-authenticated users in Tenable.sc, see [Add a SAML-Authenticated User](#).
 - To automatically add SAML-authenticated users by importing users from your SAML identity provider, see [Configure SAML User Provisioning](#).
- Instruct users to log in to Tenable.sc 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.sc by importing user accounts from your SAML identity provider. When user provisioning is enabled, users who log into your SAML identity provider are automatically created in Tenable.sc. For more information about SAML authentication in Tenable.sc, see [SAML Authentication](#).

If you enable user provisioning and a user who does not have a Tenable.sc user account logs in using your SAML identity provider, Tenable.sc automatically creates a user account for them in Tenable.sc.

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

Note: If you want to delete a Tenable.sc user that was created via SAML user provisioning, delete the user from your SAML identity provider. If you delete a user in Tenable.sc that was created via SAML user provisioning without deleting the user in your SAML identity provider, Tenable.sc automatically re-creates the user in Tenable.sc the next time they log in using your SAML identity provider.

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



Configure SAML User Provisioning

Required User Role: Administrator

You can enable user provisioning to automatically create SAML-authenticated users in Tenable.sc by importing user accounts from your SAML identity provider. When user provisioning is enabled, users who log into your SAML identity provider are automatically created in Tenable.sc. For more information, see [SAML User Provisioning](#).

To manually create SAML-authenticated users in Tenable.sc, see [Add a SAML-Authenticated User](#).

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

Before you begin:

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

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

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **System > Configuration**.

The **Configuration** page appears.

3. Click the **SAML** button.

The **SAML Configuration** page appears.

4. In the **SAML Settings** section, click the toggle to enable **User Provisioning**.
5. (Optional) To automatically update contact information for imported SAML-authenticated users, click the **User Data Sync** toggle. For more information about **User Data Sync**, see [SAML Authentication Options](#).
6. Click **Submit**.

Tenable.sc saves your configuration.

What to do next:



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

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



SAML Authentication XML Configuration Examples

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

- [OneLogin Example](#)
- [Okta Example](#)
- [Microsoft ADFS Example](#)

OneLogin Example

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

OneLogin Field	Description
Relay State	Leave this field blank.
Audience	Type <code>tenable.sc</code> .
Recipient	Type <code>https://<Tenable.sc host>/sam-1/module.php/saml/sp/saml2-acs.php/1</code> , where <code><Tenable.sc host></code> is the IP address or hostname for Tenable.sc.
ACS (Consumer) URL Validator	Type <code>-*</code> .
ACS (Consumer) URL	Type <code>https://<Tenable.sc host>/sam-1/module.php/saml/sp/saml2-acs.php/1</code> , where <code><Tenable.sc host></code> is the IP address or hostname for Tenable.sc.
Single Logout URL	Type <code>https://<Tenable.sc host>/sam-1/module.php/saml/index.php?sls</code> , where <code><Tenable.sc host></code> is the IP address or hostname for Tenable.sc.

Okta Example

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



Okta Field	Description
General	
Single Sign On URL	Type <code>https://<Tenable.sc host>/saml/module.php/saml/sp/saml2-acss.php/1</code> , where <code><Tenable.sc host></code> is the IP address or hostname for Tenable.sc.
Recipient URL	Type <code>https://<Tenable.sc host>/saml/module.php/saml/sp/saml2-acss.php/1</code> , where <code><Tenable.sc host></code> is the IP address or hostname for Tenable.sc.
Destination URL	Type <code>https://<Tenable.sc host>/saml/module.php/saml/sp/saml2-acss.php/1</code> , where <code><Tenable.sc host></code> is the IP address or hostname for Tenable.sc.
Audience Restriction	Type <code>tenable.sc</code> .
Default Relay State	Leave this field blank.
Name ID Format	Set to <code>Unspecified</code> .
Response	Set to <code>Signed</code> .
Assertion Signature	Set to <code>Signed</code> .
Signature Algorithm	Set to <code>RSA_SHA256</code> .
Digest Algorithm	Set to <code>SHA256</code> .
Assertion Encryption	Set to <code>Unencrypted</code> .
SAML Single Logout	Set to <code>Disabled</code> .
authnContextClassRef	Set to <code>PasswordProtectedTransport</code> .
Honor Force Authentication	Set to <code>Yes</code> .
SAML Issuer ID	Type <code>http://www.okta.com/\${org.externalKey}</code> .
Attribute Statements	



Okta Field	Description
FirstName	Set to Name Format: Unspecified and Value: <code>user.firstName</code> .
LastName	Set to Name Format: Unspecified and Value: <code>user.lastName</code> .
Email	Set to Name Format: Unspecified and Value: <code>user.email</code> .
username	Set to Name Format: Unspecified and one of the following: • Value: <code>user.displayName</code>, if your Tenable.sc user account usernames are full names (e.g., Jill Smith). • Value: <code>user.email</code>, if your Tenable.sc user account usernames are email addresses (e.g., jsmith@website.com). • Value: <code>user.login</code>, if your Tenable.sc 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.sc.



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.sc 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.sc to use when authenticating SAML users. For example: To transform an incoming claim: - In Incoming claim type, select Email address or UPN. - In Outgoing claim type, select Name ID. - In Outgoing name ID format, select Transient Identifier. - Select the Pass through all claim values check box. To send LDAP attributes as claim: - In Attribute store, select Active Directory. - In LDAP Attribute, select E-Mail Addresses.



Microsoft ADFS Configuration	Description
	3. In Outgoing Claim Type, select E-Mail Addresses. Note: Tenable Support does not assist with claim rules.



Certificate Authentication

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

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

Configuring certificate authentication is a multi-step process.

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

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

What to do next:

- Instruct users to log in to Tenable.sc via certificate, as described in [Log in to the Web Interface via SSL Client Certificate](#).



Configure Tenable.sc to Allow SSL Client Certificate Authentication

You must configure the Tenable.sc server to allow SSL client certificate connections. For complete information about certificate authentication, see [Certificate Authentication](#).

To allow SSL client certificate authentication:

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

Value	Description
none (default)	Tenable.sc does not accept SSL certificates for user authentication.
require	Tenable.sc requires a valid SSL certificate for user authentication.
optional	Tenable.sc accepts but does not require a valid SSL certificates for user authentication. If a user does not present a certificate, they can log in via username and password. Note: Depending on how they are configured, some web browsers may not connect to Tenable.sc when the optional setting is used.
optional_no_ca	Tenable.sc 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 if the issue is key-based or CA-based.

3. Edit the **SSLVerifyDepth** setting to specify the length of the certificate chain you want Tenable.sc to accept for user authentication. For example:



- When set to **0**, Tenable.sc accepts self-signed certificates.
- When set to **1**, Tenable.sc does not accept intermediate certificates. Tenable.sc accepts self-signed certificates or certificates signed by known CAs.
- When set to **2**, Tenable.sc accepts up to 1 intermediate certificate. Tenable.sc accepts self-signed certificates, certificates signed by known CAs, or certificates signed by unknown CAs whose certificate was signed by a known CA.

4. Save the file.

Tenable.sc saves your configuration.



Configure a CRL in Tenable.sc

Required User Role: Root user

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

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

Before you begin:

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

To configure a CRL in Tenable.sc:

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

Tenable.sc saves your configuration.

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

Tenable.sc 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.sc in a subdirectory of `/opt/sc/support/conf/`.
6. Configure Tenable.sc to trust your CA, as described in [Trust a Custom CA](#).

Tenable.sc processes your CA.

7. In the command line interface (CLI), run the following command to enable the CRL in Tenable.sc:

```
$ 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 /op-
t/sc/support/conf/crl/ca.crl
```

Tenable.sc 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.sc checks all certificates in a chain against the CRL.
leaf		Tenable.sc checks only the end-entity certificate in a chain against the CRL.
SSLCARevocationFile <filepath>		
Specifies the file path for the CRL file in Tenable.sc. For example, <code>/opt/sc/support/conf/crl/ca.crl</code> .		

- b. Save the file.

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

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

Tenable.sc restarts.



Configure OCSP Validation in Tenable.sc

Required User Role: Root user

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

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

Before you begin:

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

To configure OCSP validation in Tenable.sc:

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

Tenable.sc 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
SSLOCSPEDefaultResponder <URI>
SSLOCSPOverrideResponder on
```

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

- b. Save the file.

Tenable.sc saves your configuration.



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

Tenable.sc restarts.



Certificates and Certificate Authorities in Tenable.sc

Tenable.sc includes the following defaults:

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

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

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



Tenable.sc Server Certificates

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

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

Problem	Solution
The default certificate for Tenable.sc is untrusted.	Upload a certificate for the Tenable.sc server, as described in Upload a Server Certificate for Tenable.sc. If the new server certificate is self-signed, plugin 51192 may report that the Tenable.sc server certificate is untrusted. To configure Nessus to trust the server certificate, upload the CA certificate to Nessus.
Your browser reports that the Tenable.sc server certificate is untrusted.	Upload a CA certificate for the Tenable.sc server certificate to your browser.
Plugin 51192 reports that the Tenable.sc server certificate expired.	Regenerate the Tenable.sc server certificate, as described in Regenerate the Tenable.sc Server Certificate .



Upload a Server Certificate for Tenable.sc

Required User Role: Root user

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

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

Before you begin:

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

To upload a server certificate for Tenable.sc:

1. Log in to Tenable.sc via the user interface.
2. Back up the existing `SecurityCenter.crt` and `SecurityCenter.key` files located in the `/opt/sc/support/conf` directory.

For example:

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

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

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

If prompted, type `y` to overwrite the existing files.

4. To confirm the files have the correct permissions (640) and ownership (tns), run:

```
# 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 (640) and ownership (tns). Additionally, you must remove the # from the line in /opt/sc/support/conf/vhostssl.conf that begins with #SSLCertificateChainFile to enable the setting. Modify the path and filename to match the uploaded certificate.

If necessary, change the ownership or permissions.

- a. To change the ownership, run:

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

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

5. Restart the Tenable.sc service:

```
# service SecurityCenter restart
```

6. In a browser, log in to the Tenable.sc user interface as a user with administrator permissions.
7. When prompted, verify the new certificate details.

What to do next:

- If you uploaded a self-signed server certificate and plugin 51192 reports that the CA for your self-signed certificate is untrusted, upload the custom CA certificate to Nessus.



Regenerate the Tenable.sc Server Certificate

Required User Role: tns user

Required User Role: Root user

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

To regenerate the Tenable.sc SSL certificate:

1. Log in to Tenable.sc via the command line interface (CLI).
2. In the CLI in Tenable.sc, 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
```

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

Argument	Description
<code>-q</code>	Suppresses the warning: This script generates a self-signed SSL certificate, which is not recommended for production.
<code>-h <IP/host name></code>	Specifies an IP address or hostname that will be used as the Common Name for the certificate.

Tenable.sc generates a new certificate.

4. Run the following command to exit the `tns` user:



```
exit
```

5. As the root user, run the following command to restart the Tenable.sc service:

```
# service SecurityCenter restart
```

The service restarts and Tenable.sc applies the new certificate.



Trust a Custom CA

Required User Role: tns user

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

To configure Tenable.sc to trust a custom CA:

1. Log in to Tenable.sc via the user interface.
2. Copy the required PEM-encoded CA certificate (and intermediate CA certificate, if needed) to the Tenable.sc server's `/tmp` directory.

In this example, the file is named `ROOTCA2.cer`.

3. Run the `installCA.php` script to create the required files for each CA in `/opt/sc/data/CA`:

```
# /opt/sc/support/bin/php /opt/sc/src/tools/installCA.php /tmp/ROOTCA2.cer2
```

Tenable.sc processes all the CAs in the file.

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



System Settings

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

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



Configuration Settings

The configuration menu includes the following settings:

- [Data Expiration Settings](#)
- [External Schedules Settings](#)
- [Lumin Settings](#)
- [Mail Settings](#)
- [Miscellaneous Settings](#)
- [License Settings](#)
- [Plugins/Feed Settings](#)
- [SAML Settings](#)
- [Security Settings](#)

Data Expiration Settings

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

Option	Description
Vulnerability Data Lifetime	
Active	The number of days you want Tenable.sc to retain active scan vulnerability data stored in IP repositories. The default value of this option is 365 days.
Passive	The number of days you want Tenable.sc to retain NNM vulnerability data stored in IP repositories. The default value of this option is 7 days.
Event	The number of days you want Tenable.sc to retain LCE event data stored in IP repositories. The default value of this option is 365 days.
Compliance	The number of days you want Tenable.sc to retain audit compliance data stored in IP repositories. The default value of this option is 365 days.
Mitigated	The number of days you want Tenable.sc to retain mitigated vulnerability



Option	Description
	data. The default value of this option is 365 days.
Agent	The number of days you want Tenable.sc to retain agent scan vulnerability data stored in agent repositories. The default value of this option is 365 days.
User Generated Object Lifetime	
Closed Tickets	The number of days you want Tenable.sc to retain closed tickets. The default value of this option is 365 days.
Scan Results	The number of days you want Tenable.sc to retain scan results. The default value of this option is 365 days.
Report Results	The number of days you want Tenable.sc to retain report results. The default value of this option is 365 days.

External Schedules Settings

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

Option	Description
Nessus Network Monitor	
Pull Interval	This option configures the interval that Tenable.sc will use to pull results from the attached NNM instances. The default setting is 1 hour. The timing is based from the start of the Tenable.sc service on the host system.
Log Correlation Engine	
IDS Signatures	Frequency to update Tenable.sc IDS signatures via third-party sources. The schedule is shown along with the time zone being used.
IDS Correlation Databases	Frequency to push vulnerability information to the LCE for correlation. The schedule is shown along with the time zone being used.



Each of the update schedule times may also be configured to occur by time in a particular time zone, which can be selected via the **Time Zone** link next to each hour selection.

Lumin Settings

If you have a Tenable.io license to use Lumin with Tenable.sc, you can configure your Tenable.sc data to synchronize to Tenable.io for Lumin analysis.

For more information, see [Lumin Synchronization](#).

Mail Settings

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

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

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

Miscellaneous Settings

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

Web Proxy

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

Syslog



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

Scanning

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

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

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

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

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

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



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

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

Notifications

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

Report Generation

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.sc, 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 Consolidated ARF	Enable the DISA consolidated ARF report format, which meets the 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.



Privacy

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

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

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

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

License Settings

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

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

Plugins/Feed Settings

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

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

Update	Description
Tenable.sc Feed	Retrieves the latest Tenable.sc feed from Tenable. This feed includes data for general use, including templates (e.g., dashboards, ARCs, reports, policies, assets, and audit files), template-required objects, some general plugin information, and updated VPR values.
Active Plugins	Retrieves the latest active plugins feed (for Nessus and Tenable.io scanners)



Update	Description
	from Tenable. Tenable.sc pushes the feed to Nessus and Tenable.io scanners.
Passive Plugins	Retrieves the latest passive plugins feed from Tenable. Tenable.sc pushes the feed to NNM instances.
Event Plugins	Retrieves the latest event plugins feed from Tenable. Tenable.sc uses the feed locally with LCE data but does not push the feed to LCE; LCE retrieves the feed directly from Tenable.

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

Plugin Detail Locale

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

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

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

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

Schedules

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

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

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

SAML Settings

Use the SAML section to configure SAML 2.0 or Shibboleth 1.32.0-based SAML authentication for Tenable.sc users. For more information, see [SAML Authentication](#).

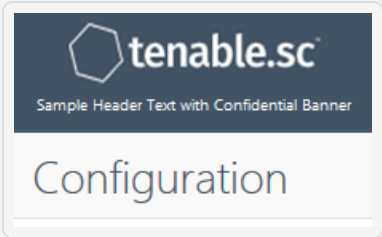
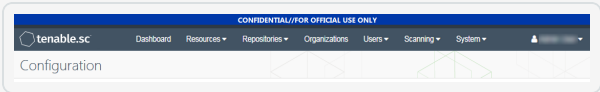
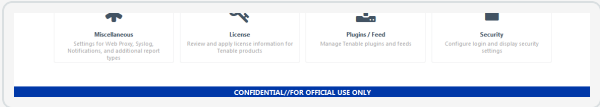


Security Settings

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

Option	Description
Authentication Settings	
Session Timeout	The web session timeout in minutes (default: 60).
Maximum Login Attempts	The maximum number of user login attempts allowed by Tenable.sc before the account is locked out (default: 20). Setting this value to 0 disables this feature.
Minimum Password Length	This setting defines the minimum number of characters for passwords of accounts created using the local TNS authentication access (default: 3).
Password Complexity	When enabled, user passwords must be at least 4 characters long and contain at least one of each of the following: • An uppercase letter • A lowercase letter • A numerical character • A special character Note: After you enable Password Complexity, Tenable.sc prompts all users to reset their passwords the next time they log in to Tenable.sc. Note: If you enable Password Complexity and set the Minimum Password Length to a value greater than 4, Tenable.sc enforces the longer password requirement.
Startup Banner Text	Type the text banner that is displayed prior to the login interface.
Header Text	Adds custom text to the top of the Tenable.sc user interface pages. The text may be used to identify the company, group, or other organizational information. The option is limited to 128 characters.



Option	Description
	
Classification Type	Adds a header and footer banner to Tenable.sc to indicate the classification of the data accessible via the software. Current options are None, Unclassified, Confidential, Secret, Top Secret, and Top Secret – No Foreign. Sample header:  Sample footer:  Note: When set to an option other than None, the available report style for users will only show the plain report style types. 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.sc 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 will appear. This feature displays the option that will allow the administrator user to set a session limit for all users.



Option	Description
Disable Inactive Users	When enabled, Tenable.sc disables user accounts after a set period of inactivity. A disabled user cannot log in to Tenable.sc, but other users can use and manage objects owned by the disabled user.
Days Users Remain Enabled	When Disable Inactive Users is enabled, specifies the number of inactive days you want to allow before automatically disabling a user account.
Session Limit	Any number entered here will be saved as the maximum number of sessions a user can have open at one time. If you log in and the session limit has already been reached, you will be prompted with a warning that the oldest session with that username will be logged out automatically. You can cancel the login, or proceed with the login and end the oldest session. Note: This behavior is different for CAC logins. The previously described behavior is bypassed as was the old login behavior.
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: It is strongly advised that the user confirm, in a separate session, that at least one user (preferably an administrator user) is able to log-in successfully via WebSEAL before the user that enabled WebSEAL logs out. Otherwise, if there is an issue, no one will be able to access Tenable.sc to turn WebSEAL off. Caution: Any user created while WebSEAL was enabled will not have a password and an admin must update the user account to establish a password. Any user that existed before the enabling of WebSEAL must revert to their old password.
PHP Serialization	
Operational Status	Summarizes your current setting.



Option	Description
PHP Serialization Mode	Specifies whether you want to allow or prevent PHP serialization in Tenable.sc. • PHP Serialization ON – Tenable.sc performs PHP serialization and Tenable.sc features operate as expected. • PHP Serialization OFF – Tenable.sc 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
Scanners	
Picture in Picture	When enabled, allows administrators to view and manage Nessus scanner configurations from the Tenable.sc user interface. For more information, see Enable Picture in Picture. Note: You cannot use Picture in Picture with a Nessus scanner if you enabled Use Proxy for the scanner or if the scanner's Authentication Type is SSL Certificate. For more information, see Nessus Scanner Settings.



Edit Plugin and Feed Settings and Schedules

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

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

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

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **System > Configuration**.

The **Configuration** page appears.

3. Click the **Plugins/Feed** button.

The **Plugins/Feed Configuration** page appears.

4. View the **Plugin Detail Locale** section to see the local language configured for Tenable.sc.
5. Expand the **Schedules** section to show the settings for the **Tenable.sc Feed**, **Active Plugins**, **Passive Plugins**, or **Event Plugins** schedule.
6. If you want to update a plugin or feed on demand, click **Update**. You cannot update feeds with invalid activation codes.
7. If you want to upload a custom feed file, click **Choose File**.
8. Click **Submit**.

Tenable.sc saves your configuration.

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

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **Username > Feeds**.

The Plugins/Feed Configuration page appears.

3. View the **Plugin Detail Locale** section to see the local language configured for Tenable.sc.



4. Expand the **Schedules** section to show the settings for the **Tenable.sc Feed**, **Active Plugins**, **Passive Plugins**, or **Event Plugins** schedule.
5. If you want to update a plugin or feed on demand, click **Update**. You cannot update feeds with invalid activation codes.
6. If you want to upload a custom feed file, click **Choose File**.
7. Click **Submit**.

Tenable.sc saves your configuration.



Configure Plugin Text Translation

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

To configure plugin text translation:

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



API Key Authentication

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

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

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

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

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

For more information about the Tenable.sc API, see the [Tenable.sc API Guide](#) and the [Tenable.sc API Best Practices Guide](#).



Enable API Key Authentication

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

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

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

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **System > Configuration**.

The **Configuration** page appears.

3. Click the **Security** tile.

The **Security Configuration** page appears.

4. In the **Authentication Settings** section, click **Allow API Keys** to enable the toggle.
5. Click **Submit**.

Tenable.sc saves your configuration.

What to do next:

- Generate API keys for a user, as described in [Generate API Keys](#).



Disable API Key Authentication

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

Caution: Disabling API keys prevents users from authenticating API requests with API keys. Disabling API keys does not delete existing API keys. If you re-enable API keys, Tenable.sc reauthorizes any API keys they were active before you disabled API key authentication.

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

To disable API key authentication:

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **System > Configuration**.

The **Configuration** page appears.

3. Click the **Security** tile.

The **Security Configuration** page appears.

4. In the **Authentication Settings** section, click **Allow API Keys** to disable the toggle.
5. Click **Submit**.

Tenable.sc saves your configuration.



Enable Picture in Picture

Required User Role: Administrator

You can enable **Picture in Picture** to allow administrators to view and manage Nessus scanner configurations from the Tenable.sc user interface.

Note: You cannot use **Picture in Picture** with a Nessus scanner if you enabled **Use Proxy** for the scanner or if the scanner's **Authentication Type** is **SSL Certificate**. For more information, see [Nessus Scanner Settings](#).

To enable **Picture in Picture**:

1. Log in to Tenable.sc via the user interface.
2. Click **System > Configuration**.

The **Configuration** page appears.

3. Click the **Security** tile.

The **Security Configuration** page appears.

4. In the **Scanners** section, click **Picture in Picture** to enable the toggle.
5. Click **Submit**.

Tenable.sc saves your configuration.

What to do next:

- View and manage your Nessus instances in Tenable.sc, as described in [View Nessus Instances in Tenable.sc](#).



Disable Picture in Picture

Required User Role: Administrator

For more information, see [Nessus Scanners](#).

To disable **Picture in Picture**:

1. Log in to Tenable.sc via the user interface.
2. Click **System > Configuration**.

The **Configuration** page appears.

3. Click the **Security** tile.

The **Security Configuration** page appears.

4. In the **Scanners** section, click **Picture in Picture** to disable the toggle.
5. Click **Submit**.

Tenable.sc saves your configuration.



Lumin Data

After you configure Tenable.sc data synchronization to Lumin in Tenable.io, you can monitor information about your Lumin metrics and past synchronizations. For general information about Lumin synchronization, see [Configure Lumin Synchronization](#).

Tenable.sc retrieves your latest Cyber Exposure Score (CES) and Assessment Maturity grade daily from Lumin in Tenable.io. For more information about the metrics and timing, see [View Lumin Metrics](#).

Tenable.sc logs all Lumin synchronization activity. For more information about the log contents, see [View Lumin Data Synchronization Logs](#).



View Lumin Metrics

Required Additional License: Tenable Lumin

Required User Role: Administrator

After you configure Tenable.sc data synchronization to Lumin in Tenable.io, you can view information about your Lumin metrics.

Every day at 11:00 PM UTC, Tenable.sc retrieves data from Lumin in Tenable.io.

Note: Newly transferred data does not immediately impact your Lumin metrics (for example, your CES). Tenable requires up to 48 hours to recalculate your metrics. Recalculated metrics appear in Tenable.sc after the next daily retrieval.

For more information, see [How long does synchronization take to complete?](#).

Tip: To view all Lumin data and take advantage of full Lumin functionality, see [Get Started with Lumin](#) in the *Tenable.io User Guide*.

To view Lumin metrics in Tenable.sc:

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **System > Lumin Data**.

The **Lumin Data** page appears.

3. In the **Metrics** section, view data about your Lumin metrics.
 - An updated [Cyber Exposure Score](#) (CES) for the data you synchronized to Lumin. High CES values indicate higher risk.
 - An updated [Assessment Maturity](#) grade for the data you synchronized to Lumin. A high grade indicates you are assessing your assets frequently and thoroughly.

If a metric changed since the last retrieval, Tenable.sc identifies if the value increased (⬆️) or decreased (⬇️).

Tip: If you performed an initial synchronization, Tenable requires up to 48 hours to calculate your Lumin metrics. Then, metrics appear in Tenable.sc after the next daily



retrieval.

For more information, see [How long does synchronization take to complete?](#)



View Lumin Data Synchronization Logs

Required Additional License: Tenable Lumin

Required User Role: Administrator

After you configure Tenable.sc data synchronization to Lumin in Tenable.io, you can view the logs for past synchronizations.

For information about monitoring Lumin synchronization status, see [View Lumin Synchronization Status](#).

To view Lumin synchronization logs:

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **System > Lumin Data**.

The **Lumin Data** page appears.



3. In the **History** section, view data about your logged activity.

Column	Description
Timestamp	The date and time of the logged activity.
Object Type	The synchronization data type: asset or repository .
Sync Type	The repository or asset synchronization type: • Cumulative repository synchronization – The initial synchronization of this repository, which included all cumulative data-base data from the repository. • Active repository synchronization – A subsequent synchronization of this repository, which included only the new or modified scan result data imported to the repository. • Static asset – A synchronization of Static Assets. • Dynamic asset – A synchronization of Dynamic Assets. • Unknown – Indicates an error occurred.
Object ID	The repository ID or asset ID. To locate the ID for an object, see View Repository Details or View Asset Details .
Transfer Duration	For repository or asset synchronizations, the length of time it took Tenable.sc to transfer your repository or asset data to Tenable.io. Note: The transfer duration does not include the time required for all data and recalculated metrics to appear in Lumin. For more information, see How long does synchronization take to complete?.
Status	The status of the repository or asset synchronization: • Error – Tenable.sc failed to transfer your data to Tenable.io. • Synchronized – Tenable.sc successfully transferred your data to Tenable.io, but all data and recalculated metrics are not yet vis-



Column	Description
	ible in Lumin. • Visible in Lumin – Tenable.sc successfully transferred your data to Tenable.io and all data and recalculated metrics are visible in Lumin. For more information about the time required for all data and recalculated metrics to appear in Lumin, see How long does synchronization take to complete?

4. To view additional details about your logged activity, click a row in the table.

Column	Description
Repository or asset Message	A message explaining the reason for the synchronization Error status.
Repository or asset Organization ID	The organization ID. To locate the ID for an organization, see View Organization Details .
Repository Scan Result ID	The scan result ID. To locate the ID for a scan result, see View Scan Result Details .



Diagnostics Settings

This page displays and creates information that assists in troubleshooting issues that may arise while using Tenable.sc.

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.sc functionality is installed. For more information, see Before You Upgrade .
Sufficient Disk Space	Indicates whether you have enough disk space to support Tenable.sc 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.sc RPM installed for your operating system. For more information, see System Requirements .
Touch Debugging	Indicates whether touch debugging is enabled. You may experience performance and storage issues if you leave touch debugging enabled for extended periods of time. For more information, see Touch Debugging .
Migration Errors	Indicates whether an error occurred during a recent Tenable.sc update.
PHP Integrity Errors	Indicates whether any PHP files have been modified from the original version included in the Tenable.sc RPM.

Diagnostics File

You can use this section to generate a diagnostics file for troubleshooting with Tenable Support. For more information, see [Generate a Diagnostics File](#).



Touch Debugging

You can use this section to enable or disable touch debugging for troubleshooting with Tenable Support. For more information, see [Enable Touch Debugging](#) and [Disable Touch Debugging](#).

Note: You may experience performance and storage issues if you leave touch debugging enabled for extended periods of time.



Generate a Diagnostics File

Required User Role: Administrator

To generate a diagnostics file for Tenable Support:

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **System > Diagnostics**.

The **Diagnostics** page appears.

3. In the **Diagnostics File** section, click **Create Diagnostics File**.

The page updates with options to configure the diagnostics file.

4. In the **General** section, if you want to omit IP addresses from the diagnostics file, click to enable the **Strip IPs from Chapters** toggle.
5. In the **Chapters** section, click the toggles to enable or disable the chapters you want to include in the diagnostics file.
6. Click **Generate File**.

The system generates a `debug.zip` file and saves it in `/opt/sc`.

What to do next:

- Share the `debug.zip` file with Tenable Support for troubleshooting.



Enable Touch Debugging

Required User Role: Administrator

You can enable touch debugs to generate logs for troubleshooting with Tenable Support.

To enable touch debugging:

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **System > Diagnostics**.

The **Diagnostics** page appears.

3. In the **Touch Debugging** section, select one or more touch debug files Tenable Support asked you to enable.
4. Click **Enable/Disable Touch Debugging**.

Tenable.sc enables the touch debug files you selected and saves one or more log files to `/opt/sc/admin/logs`.

What to do next:

- Share the files with Tenable Support.
- Disable any unneeded touch debug files, as described in [Disable Touch Debugging](#).

Note: Tenable does not recommend leaving touch debug files enabled on Tenable.sc after you send the log files to Tenable Support. You may experience performance and storage issues if you leave touch debugging enabled for extended periods of time.



Disable Touch Debugging

Required User Role: Administrator

Tenable does not recommend leaving touch debug files enabled on Tenable.sc after you send the log files to Tenable Support. You may experience performance and storage issues if you leave touch debugging enabled for extended periods of time.

For more information about touch debugging files, see [Touch Debugging](#).

To disable touch debugging:

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **System > Diagnostics**.

The **Diagnostics** page appears.

3. In the **Touch Debugging** section:
 - To remove individual touch debug files, deselect the files.
 - To remove all touch debug files, click **Deselect All**.
4. Click **Enable/Disable Touch Debugging**.

Tenable.sc disables the touch debugging files you deselected.

What to do next:

- Follow Tenable Support's instructions to manually remove old log files from `/opt/sc/admin/logs`.



Job Queue Events

Path: **System** > **Job Queue**

Job Queue is a Tenable.sc feature that displays specified events in a list for review.

You can view and sort Job Queue notifications in several ways by clicking on the desired sort column. Using the  menu next to an item, that item may be viewed for more detail or, if the job is running, the process may be killed. Killing a process should be done only as a last resort, as killing a process may have undesirable effects on other Tenable.sc processes.



System Logs

Tenable.sc logs contain detailed information about functionality to troubleshoot unusual system or user activity. You can use the system logs for debugging and for maintaining an audit trail of users who access Tenable.sc or perform basic functions (for example, changing passwords, recasting risks, or running Nessus scans).

For more information, see [View System Logs](#).



View System Logs

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

For more information, see [System Logs](#).

To view system logs:

1. Log in to Tenable.sc via the user interface.
2. Click **System** > **System Logs** (Administrator users) or **Username** > **System Logs** (Organizational users).

The **System Logs** page appears.

3. To filter the logs, see [Apply a Filter](#).

The page updates to reflect the filter you applied.



Publishing Sites Settings

Path: **System** > **Publishing Sites**

Organizations may configure publishing sites as targets to send report results to a properly configured web server or a Defense Information Systems Agency (DISA) Continuous Monitoring and Risk Scoring (CMRS) site.

Option	Description
Name	Type a name for the publishing site.
Description	Type a description of the publishing site.
Type	The method Tenable.sc 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.
URI	The target address to send the report to when completed.
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.sc 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.sc (remote repository) or between a Tenable.sc and an LCE server. This also removes the need for Tenable.sc administrators to know the administrator login or password of the remote system.

Note: The public key from the local Tenable.sc must be added to the **Keys** section of the Tenable.sc from which you wish to retrieve a repository. If the keys are not added properly, the remote repository add process prompts for the root username and password of the remote host to perform a key exchange before the repository add/sync occurs.

For more information, see [Add a Key](#), [Delete a Key](#), and [Download the Tenable.sc SSH Key](#).

Remote LCE Key Exchange

A manual key exchange between the Tenable.sc and the LCE is normally not required; however, in some cases where remote root login is prohibited or key exchange debugging is required, you must manually exchange the keys.

For the remote LCE to recognize the Tenable.sc, you need to copy the SSH public key of the Tenable.sc and append it to the `/opt/lce/.ssh/authorized_keys` file. The `/opt/lce/daemons/lce-install-key.sh` script performs this function. For more information, see [Manual LCE Key Exchange](#).



Add a Key

Required User Role: Administrator

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

To add a new key:

1. Log in to Tenable.sc via the user interface.
2. Click **System > Keys**.

The **Keys** page appears.

3. Click **Add**.

The **Add Key** page appears.

4. In the **Type** drop-down, select **DSA** or **RSA**.
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.sc.
7. Click **Submit**.

Tenable.sc saves your configuration.



Delete a Key

Required User Role: Administrator

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

To delete a key:

1. Log in to Tenable.sc via the user interface.
2. Click **System** > **Keys**.
3. In the row for the key you want to delete, click the  menu.

The actions menu appears.

4. Click **Delete**.

A confirmation window appears.

5. Click **Delete**.

Tenable.sc deletes the key.



Download the Tenable.sc SSH Key

Required User Role: Administrator

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

To download the Tenable.sc SSH key:

1. Log in to Tenable.sc via the user interface.
2. Click **System** > **Keys**.
3. In the **Options** drop-down, click **Download SC Key**.

The Tenable.sc SSH key downloads.



Username Menu Settings

The username menu in the top navigation bar contains pages to manage your user account.

Note: Depending on the screen resolution, the username may be omitted and only a user icon appears.

About

Path: **Username** > **About**

The **About** menu item displays the Tenable.sc version, Server Build ID, and copyright information.

System Logs (Organizational Users Only)

Path: **Username** > **System Logs**

For a complete discussion about system logs, see [System Logs](#).

Profile (Organizational Users Only)

Path: **Username** > **Profile**

The **Profile** option launches the **Edit User Profile** page, where you can modify some of your user account information and permissions. For more information about user account options, see [User Accounts](#).

Feeds (Organizational Users Only)

Path: **Username** > **Feeds**

The **Feeds** option displays information about the Tenable.sc feeds and plugin sets and, if permitted, a link to update the plugins either through Tenable.sc or by manually uploading plugins. The displayed feeds are for Tenable.sc Feed, Active Plugins, Passive Plugins, and Event Plugins. Only feeds with valid Activation Codes are updatable.

Plugins are scripts used by the Nessus, NNM, and LCE servers to interpret vulnerability data. For ease of operation, Nessus and NNM plugins are managed centrally by Tenable.sc and pushed out to their respective scanners. LCE servers download their own event plugins and Tenable.sc downloads



event plugins for its local reference. Tenable.sc does not currently push event plugins to LCE servers.

For more information about plugin/feed settings, see [Configuration Settings](#) and [Edit Plugin and Feed Settings and Schedules](#).

Notifications

Path: **Username** > **Notifications**

Notifications are a feature of Tenable.sc that allow specified events to display a pop-up in the lower right-hand corner of the Tenable.sc user interface.

Current notifications can be viewed by clicking on the notifications menu item.

Plugins

Path: **Username** > **Plugins**

Plugins are scripts used by the Nessus, NNM, and LCE servers to interpret vulnerability data. For ease of operation, Nessus and NNM plugins are managed centrally by Tenable.sc and pushed out to their respective scanners. LCE servers download their own event plugins and Tenable.sc downloads event plugins for its local reference. Tenable.sc does not currently push event plugins to LCE servers.

Within the Plugins interface, click the information icon next to the Plugin ID and search for specific plugins utilizing the filtering tools to view plugin details/source.

For more information about custom plugins, see [Custom Plugin Packages for NASL and CA Certificate Upload](#).

Help

Path: **Username** > **Help**

The **Help** option opens the *Tenable.sc User Guide* section for your page. To access other Tenable documentation, see <https://docs.tenable.com/>.

Logout



To end your session in Tenable.sc, click **Username** > **Logout**. Tenable recommends closing your browser window after logging out.



Custom Plugin Packages for NASL and CA Certificate Upload

You can upload a custom plugin package as a `.tar.gz` or `.tgz` file. Depending on your needs, you must include a combination of the following files:

- A `custom_feed_info.inc` file. Always include this file to time stamp your upload to Tenable.sc.
- (Optional) A `custom_nasl_archive.tar.gz` or `custom_nasl_archive.tgz` file. Include this file if you are uploading one or more custom plugins.
- (Optional) A `custom_CA.inc` file. Include this file if you are uploading one or more CA certificates to solve a Nessus scanning issue.

After you [Create the Custom Plugin Package](#) and [Upload the Custom Plugin Package](#), Tenable.sc pushes the package to Nessus for use when scanning.

Note: The system untars the files within your custom plugin package and overwrites any identically named files already in Tenable.sc or Nessus.

`custom_feed_info.inc` Guidelines

Always include this file to time stamp your upload to Tenable.sc. 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.sc.

`custom_nasl_archive.tar.gz` or `custom_nasl_archive.tgz` Guidelines

Include this file if you are uploading one or more custom plugins. This package must contain one or more custom plugin NASL files.



All custom plugins must have unique Plugin ID numbers and have family associations based on existing Tenable.sc families.

Note: Tenable Support does not assist with creating custom plugin NASL files.

custom_CA.inc Guidelines

Include this file if you are uploading one or more CA certificates to solve a Nessus scanning issue. This text file must contain PEM-encoded (Base64) CA certificate text.

For troubleshooting information, see [Troubleshooting Issues with the custom_CA.inc File](#).

One CA Certificate

If you need to include a single CA certificate, paste the PEM-encoded (Base64) certificate directly into the file.

```
-----BEGIN CERTIFICATE-----  
certificatetext  
certificatetext  
certificatetext  
certificatetext  
-----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-----
```



Create the Custom Plugin Package

Required User Role: Administrator

For complete information, see [Custom Plugin Packages for NASL and CA Certificate Upload](#).

To create the .tar.gz or .tgz custom plugin package:

1. Prepare the individual text files you want to include in the custom plugins package.

- custom_nasl_archive.tar.gz or custom_nasl_archive.tgz
- custom_feed_info.inc
- custom_CA.inc

Confirm the files meet the requirements described in [Custom Plugin Packages for NASL and CA Certificate Upload](#).

Note: After upload, the system untars the files within your custom plugin package and overwrites any identically named files already in Tenable.sc or Nessus.

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, as described in [Upload the Custom Plugin Package](#).



Upload the Custom Plugin Package

Required User Role: Administrator

For complete information, see [Custom Plugin Packages for NASL and CA Certificate Upload](#).

Before you begin:

- Create the .tar.gz or .tgz custom plugin file, as described in [Create the Custom Plugin Package](#).

Upload the .tar.gz or .tgz file to Tenable.sc:

1. Log in to Tenable.sc via the user interface.
2. Click **Username > Plugins**.

The **Plugins** page appears.

3. Click **Upload Custom Plugins** and select the .tar.gz or .tgz file.
4. Click **Submit**.

Tenable.sc uploads the package and pushes it to Nessus.

What to do next:

- To verify the upload succeeded, click **System > System Logs**.
- To verify the upload resolved a validation issue, run another scan that includes plugin 51192. Verify that Nessus has the custom plugin bundle by checking its plugin directory.



Troubleshooting Issues with the custom_CA.inc File

If uploading a custom_CA.inc file does not resolve your issue, confirm your file meets the requirements described in [custom_CA.inc Guidelines](#). Then, use these tips to continue troubleshooting.

The /opt/sc/data/customNas1/custom_CA.inc file

If the Tenable.sc installation is not on the Appliance, check the uploaded custom_CA.inc with the following command: `# cat /opt/sc/data/customNas1/custom_CA.inc`.

The output should match the custom_CA.inc file that you checked in a text editor in step T1 above. If the file does not exist, the upload was not successful. If the file does not match, the most recent upload may not have been successful. Go over the steps above for creating and uploading `upload_this.tar.gz` and ensure it is done correctly.

The /opt/nessus/lib/nessus/plugins/custom_CA.inc or \ProgramData\Tenable\Nessus\nessus\plugins\custom_CA.inc file

If Nessus is not on the Appliance, navigate to the plugins folder and `cat` or type `custom_CA.inc` to verify it exists and matches the custom_CA.inc file contents verified in steps 1 and 2 above. If `custom_CA.inc` does not exist in the plugins folder, or does not match the most recent `custom_CA.inc` in Tenable.sc, it has not propagated to the scanner. Check **Resources > Nessus Scanners** in Tenable.sc to see if the scanner is still updating plugins. If it is in a Working state, try updating the active plugins in Tenable.sc to prompt a plugin push. If the plugin feed version has not incremented and the customer must push plugins immediately, see the following article: [Force plugin update on scanner managed by Tenable.sc \(Comparable to `nessus-update-plugins -f`\)](#).

The plugin 51192 output details

Adding the custom CA certificate to custom_CA.inc does not resolve the issue if the service is missing intermediate certificate(s). If the service has a self-signed or default certificate (if not self-signed with the server name, it may be issued by a vendor name like Nessus Certification Authority) and not a certificate signed by their custom CA at all, the certificate is expired, etc.

Look at the detailed plugin output of 51192 to see exactly why the certificate is untrusted. If custom_CA.inc can fix it, the output states that the certificate at the top of the certificate chain is



unrecognized, and the certificate it shows is either issued by the custom CA (matching the name exactly) or the actual custom CA self-signed certificate.



Backup and Restore

Tenable recommends performing regular backups of the Tenable.sc data in your `/opt/sc` directory. When you restore a backup, the file overwrites the content in your `/opt/sc` directory.

Note the following limitations:

- You must restore a backup file to a Tenable.sc running the same version. For example, you cannot restore a backup file created on version 5.17.0 to a Tenable.sc running version 5.18.0.
- You must restore a backup file to the same Tenable.sc where you created the backup file. The hostname associated with the backup file must match the hostname on the receiving Tenable.sc. For example, you cannot restore a backup file created on a Tenable.sc with the hostname *Example1* to a Tenable.sc with the hostname *Example2*.

For more information, see [Perform a Backup](#) and [Restore a Backup](#).



Perform a Backup

Required User Role: Root user

For more information about the backup and restore process, see [Backup and Restore](#).

To perform a backup of Tenable.sc data:

1. Log in to Tenable.sc via the command line interface (CLI).
2. Stop Tenable.sc, as described in [Start, Stop, or Restart Tenable.sc](#).

Tenable.sc stops.

3. In the CLI in Tenable.sc, 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.sc.

5. If necessary, repeat step 4 to confirm all processes are stopped.
6. Run the following command to create a .tar file for your /opt/sc directory:

```
# tar -pzcf sc_backup.tar.gz /opt/sc
```

Note: The .tar file switches are case-sensitive.

Tenable.sc creates the backup file.

7. Run the following command to confirm the backup file is not corrupted:



```
# tar -tvf sc_backup.tar.gz
```

8. Move the backup file to a secure location.
9. Start Tenable.sc, as described in [Start, Stop, or Restart Tenable.sc](#).

Tenable.sc starts.

What to do next:

- (Optional) Restore the backup file, as described in [Restore a Backup](#).



Restore a Backup

Required User Role: Root user

For more information about the backup and restore process, see [Backup and Restore](#).

Before you begin:

- Perform a backup of your Tenable.sc, as described in [Perform a Backup](#).
- Confirm your receiving Tenable.sc meets the requirements described in [Backup and Restore](#).
- Move the backup file to your receiving Tenable.sc's /tmp directory.

To restore a backup file:

Log in to Tenable.sc via the command line interface (CLI).

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

Tenable.sc stops.

2. In the CLI in Tenable.sc, run the following command to view all running processes:

```
# ps -fu tns
```

3. 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.sc.

4. If necessary, repeat step 4 to confirm all processes are stopped.
5. Run the following commands to decompress the .tar file and overwrite the existing /opt/sc directory:



```
# cd /
```

```
# tar -xvf /tmp/sc_backup.tar.gz
```

Note: The .tar file switches are case-sensitive.

The restore finishes.

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

Tenable.sc starts.



Lumin Synchronization

You can use Tenable Lumin to quickly and accurately assess your Cyber Exposure risk and compare your health and remediation performance to other Tenable customers in your Salesforce industry and the larger population. Lumin correlates raw vulnerability data with asset business criticality and threat context data to support faster, more targeted analysis workflows than traditional vulnerability management tools. For more information about Lumin, see [Lumin](#) in the *Tenable.io User Guide*.

After you acquire a Tenable.io Lumin license for use with Tenable.sc, you can configure Tenable.sc synchronization to send limited Tenable.sc data to Tenable.io for use in Lumin analysis. Tenable.sc communicates with Tenable.io using an encrypted connection, as described in [Encryption Strength](#).

When you send data to Tenable.io, the system does not remove the data from your Tenable.sc. You can continue normal operation of Tenable.sc.

For more information, see:

- [Plan Your Lumin Synchronization](#)
- [Configure Lumin Synchronization](#)
- [View Lumin Synchronization Status](#)
- [View Lumin Data Synchronization Logs](#)
- [View Lumin Metrics](#)
- [Disable Lumin Synchronization](#)



Plan Your Lumin Synchronization

Tenable recommends planning your synchronization strategy to accommodate synchronization limitations and limit data duplication in Tenable.io.

Can I communicate with Tenable.io through a proxy?

To use the proxy configured for your Tenable.sc instance for communications with your Tenable.io instance, contact Tenable Support.

Can I synchronize multiple Tenable.sc instances?

You can synchronize data from one Tenable.sc to one Tenable.io instance. You cannot synchronize data from multiple Tenable.sc instances to a single Tenable.io instance.

If you purchase multiple Tenable.io instances, you can synchronize one Tenable.sc to each Tenable.io instance.

What data does synchronization include?

Tenable.sc supports synchronizing:

- IPv4 addresses within dynamic assets and IPv4 addresses within static assets.

Note: You cannot synchronize IPv6 addresses within static assets. If an asset contains a mix of IPv4 and IPv6 addresses, Tenable.sc synchronizes only the IPv4 addresses.

Note: You cannot synchronize non-IPv4 assets within dynamic assets. If a dynamic asset contains other asset types, Tenable.sc synchronizes only the IPv4 addresses.

Note: You cannot synchronize DNS name list assets, LDAP query assets, combination assets, watchlist assets, or import assets.

- Active or agent cumulative database and scan result vulnerability data stored in IPv4 and agent repositories.

The initial synchronization includes all cumulative database data from the repository. All subsequent synchronizations include only the new or modified scan result data imported to the repository.



Note: You cannot synchronize passive scan result vulnerability data. Tenable.sc identifies vulnerability data by plugin family and excludes NNM and LCE plugin families from synchronization.

Caution: To avoid data merge issues in Tenable.io, Tenable recommends resolving all repository overlaps before synchronizing data to Tenable.io. You cannot resolve data merge issues after synchronizing a repository with Tenable.io; you must resolve overlapping repositories in Tenable.sc before synchronizing a repository for the first time. For more information, see [Repository Overlap](#).

Do I need to synchronize both data types (repositories and assets)?

Yes. In order to accurately assess your Cyber Exposure risk with Lumin, you must synchronize one or more asset lists and one or more repositories containing vulnerability data for those assets.

How long does synchronization take to complete?

Vulnerability and asset data synchronize differently to Tenable.io.

Data	Synchronization Method	Timing
Vulnerability data	• Manual initial synchronization. • Automatic subsequent synchronizations when new scan result data imports to your synchronized repositories.	After you initiate a synchronization, Tenable.sc immediately begins transferring data to Tenable.io. After 10-15 minutes, data begins appearing in Tenable.io. Newly transferred data does not immediately impact your Lumin metrics (for example, your CES). Tenable requires up to 48 hours to recalculate your metrics.
Asset data (tags in Tenable.io)	• Manual initial synchronization. • On-demand, automatic, or scheduled subsequent synchronizations, depending on your synchronization configuration.	All data and recalculated Lumin metrics appear in Tenable.io within 48 hours. Recalculated metrics appear in Tenable.sc after the next daily retrieval.



To monitor the success or failure of synchronizations, see [View Lumin Synchronization Status](#) and [View Lumin Data Synchronization Logs](#).

Which of my synchronized assets count toward my Tenable.io license?

Synchronized assets that count toward your Tenable.sc license also count toward your Tenable.io license. For more information about Tenable.sc asset counting, see [License Requirements](#).

Where will I see synchronized data in Tenable.io?

Tip: Viewing vulnerability data is temporarily not possible in Tenable.io. You can view asset and solutions data, but not vulnerability data. For more information, contact your Tenable representative.

You can view your synchronized data in both the Vulnerability Management and Lumin areas of Tenable.io.

Vulnerability Management

View your synchronized data on the **Assets** page. For more information, see [View Assets in Tenable.io Vulnerability Management](#).

Lumin

View your synchronized data on any Lumin page. For more information, see [Get Started with Lumin](#) in the *Tenable.io User Guide*.

Tip: To view limited metrics Tenable.sc retrieves from Lumin in Tenable.io, see [View Lumin Metrics](#).



Repository Overlap

Two or more IPv4 repositories *overlap* if their specified **IP Ranges** contain intersecting IP addresses. To avoid data merge issues in Tenable.io, Tenable recommends resolving all repository overlaps before synchronizing data to Tenable.io.

To resolve an overlap between two repositories, edit the repository configurations and reconfigure the **IP Ranges** to avoid intersecting IP addresses, as described in [IPv4/IPv6 Repositories](#).

Caution: You cannot resolve data merge issues after synchronizing a repository with Tenable.io; you must resolve overlapping repositories in Tenable.sc before synchronizing a repository for the first time.

If you cannot resolve all overlaps, plan to synchronize a limited number of repositories to avoid conflicts. For example, to avoid a conflict between two repositories, synchronize one repository but not the other repository.



Configure Lumin Synchronization

Required Additional License: Tenable Lumin

Required Tenable.sc User Role: Administrator

Required Tenable.io User Role: Administrator

You can configure Tenable.sc to send limited Tenable.sc data to Tenable.io for use in Lumin analysis. For more information, see [Lumin Synchronization](#).

Before you begin:

- License and enable Lumin in Tenable.io, as described in [License and Enable Lumin](#) in the *Tenable.io User Guide*.
- Plan your synchronization strategy and review known limitations and dependencies, as described in [Plan Your Lumin Synchronization](#).
- Review your repositories for overlapping IP addresses. To avoid data merge issues in Tenable.io, Tenable recommends resolving all repository overlaps before synchronizing data to Tenable.io. For more information, see [Repository Overlap](#).

Caution: You cannot resolve data merge issues after synchronizing a repository with Tenable.io; you must resolve overlapping repositories in Tenable.sc before synchronizing a repository for the first time.

- Generate Tenable.io API keys for a Tenable.io user with Administrator permissions, as described in [Generate API Keys](#) in the *Tenable.io User Guide*.
- Share any assets you want to synchronize with the **Full Access** group, as described in [Groups](#). You cannot synchronize assets with more limited sharing.

To configure data synchronization between Tenable.sc and Lumin in Tenable.io:

1. Log in to Tenable.sc via the user interface.
2. Click **System > Configuration**.

The **Configuration** page appears.

3. Click the **Lumin** tile.



The **Lumin Configuration** page appears.

4. In the **Tenable.io Connection Settings** section, type an **Access Key** and **Secret Key** for the Tenable.io user you want to have full access to your data in Tenable.io.

Option	Description
Access Key	The Tenable.io API access key for a Tenable.io user with Administrator permissions.
Secret Key	The Tenable.io API secret key for a Tenable.io user with Administrator permissions.

Tenable.sc validates the connection to Tenable.io and locks the key configuration.

5. (Optional) To test the connection to Tenable.io, click **Test Connection**.

Tenable.sc tests the connection to Tenable.io using the access key and secret key you provided.

Tenable.sc displays a notification indicating the status of the connection to Tenable.io.

6. In the **Vulnerability Data Synchronization** section:
 - a. Select one or more IPv4 or agent repositories that contain the scan result data you want to synchronize with Tenable.io.

The initial synchronization includes all cumulative database data from the repository. All subsequent synchronizations include only the new or modified scan result data imported to the repository.

Note: You cannot synchronize passive scan result vulnerability data. Tenable.sc identifies vulnerability data by plugin family and excludes NNM and LCE plugin families from synchronization.

Caution: To avoid data merge issues in Tenable.io, Tenable recommends resolving all repository overlaps before synchronizing data to Tenable.io. You cannot resolve data merge issues after synchronizing a repository with Tenable.io; you must resolve overlapping repositories in Tenable.sc before synchronizing a repository for the first time. For more information, see [Repository Overlap](#).



Tip: Hover over the  to view [details](#) for a repository (including information about unresolved repository overlaps).

- b. Click **Synchronize**.

A confirmation window appears.

- c. Click **Synchronize**.

Tenable.sc begins synchronizing your vulnerability data to Tenable.io.

7. In the **Asset to Tag Synchronization** section:

- a. If you want to synchronize asset data at a scheduled time:

- i. Click to enable the **Custom Schedule** slider.
- ii. Next to the schedule link, click the  button.
- iii. Modify the **Time** and **Timezone** options to specify when you want synchronizations to occur.

Tip: You cannot modify the **Frequency** or **Repeat Every** options; all Lumin synchronizations occur once daily.

If you do not schedule your asset synchronizations, Tenable.sc automatically synchronizes once daily, after business hours for your local time zone.

- b. If you want to filter the assets that appear in the **Unstaged Assets** section, do any of the following:

- Select an organization from the **Organization Filter** drop-down list and click **Apply Filters**.
- Select an asset type from the **Asset Type Filter** drop-down list and click **Apply Filters**.
- Type an asset name in the **Search Name** box and press **Enter**.

Note: You can synchronize any assets shared with the **Full Access** group. You cannot synchronize assets with more limited sharing.



Tenable.sc applies your filter to the **Unstaged Assets** section.

c. To stage one or more assets for synchronization, do one of the following:

- Click the **Add All** button to stage all visible assets for synchronization.

Tenable.sc stages all visible assets for synchronization and displays them in the **Staged Assets** section.

- In the rows for individual assets you want to stage for synchronization, click the **+** button.

Tenable.sc stages your selected assets for synchronization and displays them in the **Staged Assets** section.

Note: You cannot synchronize IPv6 addresses within static assets. If an asset contains a mix of IPv4 and IPv6 addresses, Tenable.sc synchronizes only the IPv4 addresses.

Note: You cannot synchronize non-IPv4 assets within dynamic assets. If a dynamic asset contains other asset types, Tenable.sc synchronizes only the IPv4 addresses.

Note: You cannot synchronize DNS name list assets, LDAP query assets, combination assets, watchlist assets, or import assets.

Tip: Click an asset row to view [details](#) for an asset.

d. Click **Synchronize Staged Assets**.

A confirmation window appears.

e. Click **Synchronize**.

Tenable.sc begins synchronizing your assets to Tenable.io.

8. Wait for data transfer and Lumin data calculations to complete. For more information, see [How long does synchronization take to complete?](#)

9. Monitor the synchronization and confirm there were no errors, as described in [View Lumin Synchronization Status](#) or [View Lumin Data Synchronization Logs](#).

What to do next:



- Begin using Tenable.io and Lumin, as described in [Where will I see synchronized data in Tenable.io?](#).
- View Lumin metrics information within Tenable.sc, as described in [View Lumin Metrics](#).
- By default, synchronized data is visible to the Tenable.io Administrator account used for synchronization and to all other users in Tenable.io. If you want to restrict privileges for synchronized data, configure access groups as described in [Access Groups](#) in the *Tenable.io User Guide*.



View Lumin Synchronization Status

Required Additional License: Tenable Lumin

Required User Role: Administrator

After you configure Tenable.sc data synchronization to Lumin in Tenable.io, you can view the status of your synchronizations.

For information about viewing logs for past synchronizations, see [View Lumin Data Synchronization Logs](#).

Before you begin:

- Configure Lumin synchronization, as described in [Configure Lumin Synchronization](#).

To monitor the status of your data synchronization between Tenable.sc and Lumin in Tenable.io:

1. Log in to Tenable.sc via the user interface.
2. Click **System > Configuration**.

The **Configuration** page appears.

3. Click the **Lumin** tile.

The **Lumin Configuration** page appears.

4. In the **Vulnerability Data Synchronization** section:
 - View the **Last Successful Sync** date and time for data from any repository.
 - View details for a repository by hovering over the ⓘ that appears when you hover over a repository name:

Data	Description
Name	The repository name.
Format	The repository type: IPv4 or Agent .



Data	Description
First Successful Synchronization	The date and time of the first synchronization of this repository.
Last Successful Synchronization	The date and time of the most recent synchronization of this repository.
Error Status	If the most recent synchronization of this repository failed, a description of the failure.
Last Failed Synchronization	The date and time of the most recent failed synchronization of this repository.
Repositories Overlapping with <Repository Name>	The names of other repositories with IP Ranges that overlap this repository. For more information, see Repository Overlap .

5. In the **Asset to Tag Synchronization** section:

- In the **Unstaged Assets** or **Staged Assets** section, click an asset row to view details for an asset:

Data	Description
Description	The asset description.
First Sync Success	The date and time of the first synchronization of this asset.
Last Sync Success	The date and time of the most recent synchronization of this asset.
Last Sync Failure	The date and time of the most recent failed synchronization of this asset.
Sync Error	If the most recent synchronization of this asset failed, a description of the failure.

- View the **Last Successful Sync** date and time for any asset data.



Disable Lumin Synchronization

Required Additional License: Tenable Lumin

Required User Role: Administrator

When you disable Lumin synchronization, Tenable.sc stops synchronizing new or updated scan result and asset data with Lumin in Tenable.io. Existing Tenable.sc data remains visible in Tenable.io.

To stop synchronizing data with Lumin in Tenable.io:

1. Log in to Tenable.sc via the user interface.
2. Click **System > Configuration**.

The **Configuration** page appears.

3. Click the **Lumin** tile.

The **Lumin Configuration** page appears.

4. In the **Vulnerability Data Synchronization** section:
 - a. Deselect all of your repositories.
 - b. Click **Synchronize**.

Tenable.sc stops synchronizing vulnerability data to Tenable.io. Existing Tenable.sc data remains visible in Tenable.io.

5. In the **Asset to Tag Synchronization** section:
 - a. In the **Staged Assets** section, click **Remove All**.

All staged assets move to the **Unstaged Assets** section.

- b. Click **Synchronize Staged Assets**.

Tenable.sc stops synchronizing asset data to Tenable.io. Existing Tenable.sc data remains visible in Tenable.io.



Configure Scans

See the following sections to configure Tenable.sc scans.

- [Scanning Overview](#)
- [Resources](#)
- [Repositories](#)
- [Active Scans](#)
- [Active Scan Objects](#)
- [Agent Scans](#)
- [Agent Scanning](#)
- [Blackout Windows](#)
- [Patch Management](#)



Scanning Overview

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

Configuring both methods provides a comprehensive view of the organization's security posture and reduces false positives. For more information about Tenable scanning strategies, see the [Tenable Scan Strategy Guide](#).

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 NNM 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 <i>authenticated</i> or <i>unauthenticated</i> active scan using a Nessus or Tenable.io scanner. • an agent scan using an agent-capable Tenable.io or 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.	In general, assets assessed by assessment scans count toward your license.



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

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

Unauthenticated Active Scans

If you do not add access credentials to your assessment scan configuration, Tenable.io performs a limited number of checks when scanning your assets.

For more information about how discovered and assessed assets are counted towards your license, see [License Requirements](#).



Resources

Administrator users can configure supporting resources.

- [Nessus Scanners](#)
- [Nessus Network Monitor Instances](#)
- [Log Correlation Engines](#)
- [Log Correlation Engine Clients](#)
- [Log Correlation Engine Client Policies](#)
- [Tenable.ot Instances](#)

Scan zone resources are considered active scan objects. For more information, see [Active Scan Objects](#) and [Scan Zones](#).

LDAP server resources are part of user account configuration. For more information, see [User Accounts](#) and [LDAP Authentication](#).



Nessus Scanners

For high level information about active and agent scanning, see [Active Scans](#) and [Agent Scans](#).

In the Tenable.sc framework, the Nessus scanner behaves as a server, while Tenable.sc serves as a client that schedules and initiates scans, retrieves results, reports results, and performs a wide variety of other important functions.

You can add Nessus or Tenable.io deployments to Tenable.sc as Nessus scanners in Tenable.sc:

- Managed or unmanaged Nessus scanners

Note: Tenable.sc cannot perform scans with or update plugins for scanners running unsupported versions of Nessus. For minimum Nessus scanner version requirements, see the [Tenable.sc Release Notes](#) for your version.

- Nessus Manager instances

Note: If you enabled clustering on Nessus Manager, add the parent node of the cluster to Tenable.sc. For more information, see [Clustering](#) in the *Nessus User Guide*.

- Tenable.io instances

For more information, see:

- [Add a Nessus Scanner](#)
- [Add a Tenable.io Scanner](#)
- [Manage Nessus Scanners](#)
- [View Your Nessus Scanners](#)
- [View Details for a Nessus Scanner](#)
- [Delete a Nessus Scanner](#)
- [View Nessus Instances in Tenable.sc](#)

For information about Tenable.sc-Nessus and Tenable.sc-Tenable.io communications encryption, see [Encryption Strength](#).

Nessus Scanner Settings



Option	Description
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.sc. The default is port 8834.
Enabled	A scanner may be Enabled or Disabled within Tenable.sc to allow or prevent access to the 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. Note: Confirm that the correct CA certificate is configured for use by Tenable.sc. If you are using a custom CA, configure Tenable.sc to trust your custom CA, as described in Trust a Custom CA. You do not need to perform this step when using the default certificates for Nessus servers.
Use Proxy	Instructs Tenable.sc to use its configured proxy for communication with the scanner.
Authentication Type	Select Password or SSL Certificate for the authentication type to connect to the scanner. For complete information about 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.sc, 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



Option	Description
	available if the Authentication Type is set to Password .
Certificate	If you set Authentication Type to SSL Certificate, specifies the <code>nes-suscert.pem</code> file you want to use for authentication to the scanner. For complete information about Nessus SSL certificate authentication, see Manual Nessus SSL Certificate Exchange.
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.
Zones	The scan zones that can use this scanner. For more information, see Scan Zones .
Agent Capable	Specifies whether you want this scanner to provide Nessus Agent scan results to Tenable.sc. Agent capable scanners must be either Tenable.io or Nessus Manager 6.5 or later. When using Nessus Manager, you must use an organizational user account to connect from Tenable.sc.
Organizations	When the Agent Capable option is enabled, specifies one or more organizations that you want to grant access to import Nessus Agent data into Tenable.sc.
API Keys	When the Agent Capable option is enabled, specifies whether you want to use secure API keys when importing agent scan data from Nessus or Tenable.io scanners. For more information about retrieving your access key and secret key from Nessus and Tenable.io, see Generate a Nessus API Key in the <i>Nessus User Guide</i> and Generate a Tenable.io API Key in the <i>Tenable.io User Guide</i>.
Access Key	When the API Keys option is enabled, specifies the access key for the Nessus or Tenable.io scanner.



Option	Description
Secret Key	When the API Keys option is enabled, specifies the secret key for the Nessus or Tenable.io scanner.



Add a Nessus Scanner

Required User Role: Administrator

For more information, see [Nessus Scanners](#).

Note: Tenable.sc cannot perform scans with or update plugins for scanners running unsupported versions of Nessus. For minimum Nessus scanner version requirements, see the [Tenable.sc Release Notes](#) for your version.

To add a Nessus scanner to Tenable.sc:

1. Log in to Tenable.sc via the user interface.
2. Click **Resources** > **Nessus Scanners**.

The **Nessus Scanners** page appears.

3. Click **Add**.

The **Add Nessus Scanner** page appears.

4. Configure Nessus scanner options, as described in [Nessus Scanners](#).
 - a. In the **Name** box, type a name for the scanner.
 - b. In the **Description** box, type a description for the scanner.
 - c. In the **Host** box, type the hostname or IP address for the scanner.
 - d. In the **Port** box, view the default (**8834**) and modify, if necessary.
 - e. If you want to disable this scanner's connection to Tenable.sc, click **Enabled** to disable the connection.
 - f. 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 Nessus scanner, click **Verify Hostname** to enable the toggle.
 - g. If you want to use the proxy configured in Nessus for communication with the scanner, click **Use Proxy** to enable the toggle.
 - h. In the **Type** drop-down box, select the authentication type.



- i. If you selected **Password** as the **Type**:
 - i. In the **Username** box, type the username for the account generated during the Nessus installation for daemon-to-client communications.
 - ii. In the **Password** box, type the password associated with the username you provided.
- j. 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. For more information, see [Manual Nessus SSL Certificate Exchange](#).
 - 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.
- k. Check the box for all active scan zones you want to use this scanner.
- l. If you want this scanner to provide Nessus Agent scan results to Tenable.sc:
 - 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 Nessus Agent data into Tenable.sc.
 - iii. If you want to use secure API keys when importing agent scan data from 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.sc saves your configuration.

What to do next:

- Configure a scan zone, repository, and active scan objects, as described in [Active Scans](#).



Add a Tenable.io Scanner

Required User Role: Administrator

Tenable.sc supports the use of Tenable.io as a Nessus scanner within Tenable.sc. Tenable.io is an enterprise-class remote vulnerability scanning service that may be used to audit internet-facing IP addresses for both network and web application vulnerabilities from the cloud. While they are not managed by Tenable.sc (e.g., plugins are not pushed from Tenable.sc to the scanner), Tenable.io scanners can be added to Tenable.sc in the same manner that internal, local, or remote Nessus scanners are added.

Before you begin:

- Confirm that you have a valid, active Tenable.io subscription.

To add Tenable.io to Tenable.sc as a Nessus scanner:

1. Log in to Tenable.sc via the user interface.
2. Click **Resources** > **Nessus Scanners**.
3. Click **Add**.



Add Nessus Scanner

← Back

General

Name*

Nessus Cloud

Description

Host*

cloud.tenable.com

Port*

443

Enabled

☒

Verify Hostname

☐

Use Proxy

☐

Authentication

Type

Password ▾

Username*

username@example.com

Password*

••••••••••

Active Scans

Zones

Search

Q

☐ Default Scan Zone

Agents

Agent Capable

☐

Submit

Cancel

4. Configure Nessus scanner options, as described in [Nessus Scanners](#). You must configure all required options and use Tenable.io-specific values for some settings:



Option	Value for a Tenable.io Configuration
Host	• Commercial Tenable.io: <i>cloud.tenable.com</i> • Tenable.io FedRAMP: <i>fedcloud.tenable.com</i>
Port	443
Username	The username for an active Tenable.io user account.
Password	The password for an active Tenable.io user account.
Zones	The zones within Tenable.sc that use Tenable.io as a scanner.

5. Click **Submit**.

Note: Existing scan reports from Tenable.io are not automatically available in Tenable.sc. However, you can manually download and import them into Tenable.sc.

Note: By default, Tenable.io selects the corresponding regional scanner. For example, if you run a scan in the United States, Tenable.io selects the United States scanner. If you run a scan in Germany, Tenable.io selects the Germany scanner.

What to do next:

- Configure a scan zone, repository, and active scan objects, as described in [Active Scans](#).



Nessus Scanner Statuses

You can view the status for scanners, as described in [View Your Nessus Scanners](#).

Status	Description	Recommended Action
Authentication Error	Tenable.sc could not authenticate to the scanner using the credentials you provided.	Check your scanner configuration settings and confirm the Username and Password options specify valid login credentials for the scanner.
Certificate Mismatch	Tenable.sc 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. • (Nessus scanners only) Check your scanner configuration settings and confirm the Certificate option specifies the correct <code>nessuscert.pem</code> file. For more information about managing SSL certificates in Nessus, see Manage SSL Certificates in the <i>Nessus User Guide</i>.
Connection Error	Tenable.sc 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.sc and the scanner are configured to permit network traffic.
Connection	Tenable.sc connected to	Contact your network administrator for



Timeout	the scanner but timed out waiting for a reply.	troubleshooting assistance.
Invalid Configuration	The scanner attempted to connect to a scanner on port 0.	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 .
Plugins Out of Sync	The plugin sets on the scanner do not match the plugin sets in Tenable.sc.	For troubleshooting assistance, see the knowledge base article.
Protocol Error	Tenable.sc connected to the scanner but the scanner returned an HTTPS protocol negotiation error.	Contact your network administrator for troubleshooting assistance.
Reloading Scanner	The scanner is temporarily unable to run scans because Nessus is restarting on the scanner.	None.
Updating Plugins	Tenable.sc 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.
Updating Status	Tenable.sc is refreshing the status of the scanner. Scanners can continue to run scans while Ten-	None.



	able.sc refreshes the status. Note: Tenable.sc 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.sc refreshes the status of the scanner on demand.	
User Disabled	A Tenable.sc 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 Nessus Scanners.
Working	The scanner is connected to Tenable.sc and able to run scans.	None.



Manage Nessus Scanners

Required User Role: Administrator

For more information, see [Nessus Scanners](#).

To manage your Nessus scanners:

1. Log in to Tenable.sc via the user interface.
2. Click **Resources** > **Nessus Scanners**.

The **Nessus Scanners** page appears.

3. To filter the scanners that appear on the page, apply a filter as described in [Apply a Filter](#).
4. To view the list of configured scanners, see [View Your Nessus Scanners](#).
5. To view details for a scanner, see [View Details for a Nessus Scanner](#).

6. To edit a scanner:

- a. In the row for the scan, click the  menu.

The actions menu appears.

- b. Click **Edit**.

The **Edit Nessus Scanner** page appears.

- c. Modify the scanner options. For more information about scanner options, see [Nessus Scanners](#).

- d. Click **Submit**.

7. To download logs for a scanner, see [Download Nessus Scanner Logs](#).
8. To delete a scanner, see [Delete a Nessus Scanner](#).



View Your Nessus Scanners

Required User Role: Administrator

For more information, see [Nessus Scanners](#).

To view a list of configured Nessus scanners:

1. Log in to Tenable.sc via the user interface.
2. Click **Resources** > **Nessus Scanners**.

The **Nessus Scanners** page appears.

3. View details about each Nessus scanner.
 - **Name** — The name for the scanner.
 - **Features** — Specifies whether the scanner is a **Standard** scanner or an **Agent Capable** scanner. Agent capable scanners provide Nessus Agent scan results to Tenable.sc.
 - **Status** — The status of the scanner. For more information, see [Nessus Scanner Statuses](#).
 - **Host** — The IP address or hostname of the scanner.
 - **Version** — The scanner's Nessus version.
 - **Type** — The type of scanner connection.

Type	Description
Unknown	Tenable.sc could not identify the scanner.
Nessus (Unmanaged Plugins)	Tenable.sc accesses the scanner using a Nessus user account with Standard permissions. Tenable.sc cannot send plugin updates to the scanner or manage the scanner's activation code.
Nessus (Managed Plugins)	Tenable.sc manages the scanner and authenticates via a Nessus user account.



Type	Description
	Tenable.sc sends plugin updates to the scanner and manages the scanner's activation code.
Tenable.io (Unmanaged Plugins)	Tenable.sc accesses the instance using a Tenable.io user account with Standard permissions. Tenable.sc cannot send plugin updates to the instance or manage the instance's activation code.

- **Uptime** — The length of time, in days, that the scanner has been running.
- **Last Modified** — The date and time the scanner was last modified.

4. To view details of a specific Nessus scanner, see [View Details for a Nessus Scanner](#).
5. To filter the scanners that appear on the page, apply a filter as described in [Apply a Filter](#).
6. To manually refresh the **Status** data, in the **Options** drop-down box, click **Update Status**.

Tenable.sc refreshes the **Status** data.



View Details for a Nessus Scanner

Required User Role: Administrator

For more information, see [Nessus Scanners](#).

To view details for a Nessus scanner:

1. Log in to Tenable.sc via the user interface.
2. Click **Resources** > **Nessus Scanners**.

The **Nessus Scanners** page appears.

3. In the row for the scanner for which you want to view details, click the  menu.

The actions menu appears.

4. Click **View**.

The **View Nessus Scanner** page appears.

Section	Action
Options drop-down box	• To edit the scanner, click Edit. • To delete the scanner, click Delete, as described in Delete a Nessus Scanner. • To download logs for the scanner, click Download Logs. For more information, see Download Nessus Scanner Logs.
General	View general information about the scanner.
Authentication	View authentication information for the scanner.
Active Scans	View active scan information for the scanner.
Agents	View agent information for the scanner. • Agent Capable — Specifies whether the scanner is agent capable: Yes or No.



Section	Action
	• Organizations — If the scanner is agent capable, the 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.sc refreshes the load information every 15 minutes.
Nessus Scanner Health	If you are viewing details for a managed Nessus scanner running version 8.2.0 or later, view scanner health summary data: • Running Scans — The number of scans currently running on the scanner. • Hosts Being Scanned — The number of hosts currently being scanned by the scanner. • CPU Load — The percent of the total CPU currently in use by the scanner. • Total Memory — The total memory installed on the scanner. • Memory Used — The percent of the total memory currently in use by the scanner. • Total Disk Space — The total disk space installed on the scanner. • Disk Space Used — The percent of the total disk space currently in use by the scanner. • Last Updated — The date and time Tenable.sc last updated the scanner data. Tenable.sc refreshes the data when you load the View Nessus Scanner page. To force a manual refresh, click the  button.



View Nessus Instances in Tenable.sc

Required User Role: Administrator

Administrators can view and manage Nessus scanner configurations from the Tenable.sc user interface. For more information about Nessus scanners in Tenable.sc, see [Nessus Scanners](#).

Note: You cannot use **Picture in Picture** with a Nessus scanner if you enabled **Use Proxy** for the scanner or if the scanner's **Authentication Type** is **SSL Certificate**. For more information, see [Nessus Scanner Settings](#).

Before you begin:

- Enable **Picture in Picture**, as described in [Enable Picture in Picture](#).

To view Nessus instances inside the Tenable.sc user interface:

1. Log in to Tenable.sc via the user interface.
2. Click **Resources** > **Nessus Scanners**.

The **Nessus Scanners** page appears.

3. In the row for the Nessus scanner, click the  menu.

The actions menu appears.

4. Click **Manage System**.

The Nessus instance opens inside the Tenable.sc user interface.

What to do next:

- Manage your Nessus scanner configurations using the picture in picture window in Tenable.sc. For more information about Nessus and Nessus settings, see the *Nessus User Guide*.



Download Nessus Scanner Logs

Required User Role: Administrator

You can download a log file for Nessus scanners managed by Tenable.sc. The Nessus scanner must be running version 8.0.0 or later to send logs to Tenable.sc for download.

All Nessus scanner logs include:

- Recent Nessus log data
- System information (operating system version, CPU statistics, available memory, available disk space, etc.)
- Troubleshooting data

If you include extended logs, the system also downloads recent Nessus web server log records, system log data, and network configuration information.

To download logs for a Nessus scanner:

1. Log in to Tenable.sc via the user interface.
2. Click **Resources > Nessus Scanners**.

The **Nessus Scanners** page appears.

3. In the row for the scanner for which you want to download logs, click the  menu.

The actions menu appears.

4. Click **Download Logs**.

The **Download Nessus Scanner Logs** window appears.

5. To include recent Nessus web server log records, system log data, and network configuration information, click to enable the **Extended Logs** toggle.
6. To hide the first two octets of IPv4 addresses within the logs, click to enable the **Sanitize IPs** toggle.
7. Click **Download**.

Tenable.sc downloads the `tar.gz` file in your browser.



Tip: If you use 7-Zip to extract the `tar.gz` file, you may see the following error message: There are some data after the end of the payload data. You can safely ignore this error.



Delete a Nessus Scanner

Required User Role: Administrator

For more information, see [Nessus Scanners](#).

To delete a Nessus scanner:

1. Log in to Tenable.sc via the user interface.
2. Click **Resources** > **Nessus Scanners**.

The **Nessus Scanners** page appears.

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

The actions menu appears.

4. Click **Delete**.

A confirmation window appears.

5. Click **Delete**.

Tenable.sc deletes the scanner.



Nessus Network Monitor Instances

Nessus Network Monitor (NNM) is a patented network discovery and vulnerability analysis software solution that delivers real-time network profiling and monitoring for continuous assessment of an organization's security posture in a non-intrusive manner. NNM monitors network traffic at the packet layer to determine topology, services, and vulnerabilities. Where an active scanner takes a snapshot of the network in time, NNM behaves like a security motion detector on the network.

Tenable.sc communicates with NNM utilizing the XMLRPC protocol on port 8835 by default. For information about Tenable.sc-NNM communications encryption, see [Encryption Strength](#).

Note: It is important for you to restrict the data NNM collects to only the desired IP address ranges. For example, if your attached NNM collects information on 1100 hosts and Tenable.sc is licensed for 1000 hosts, Tenable.sc imports all of the NNM data and indicates that you exceeded your host count. For more information, see [License Requirements](#).

Tenable.sc will ask NNM for the latest (if any) vulnerability report once every hour by default. The pull interval may be changed under the System Configuration page under the Update tab.

To fully configure passive scan data retrieval from NNM:

1. Configure NNM, as described in [Get Started](#) in the *Nessus Network Monitor User Guide*.
2. Add your NNM license to Tenable.sc, as described in [Apply a New License](#).
3. Add an IPv4 or IPv6 repository for NNM data in Tenable.sc, as described in [Add a Repository](#).
4. Add an NNM instance in Tenable.sc, as described in [Add an NNM Instance](#).
5. (Optional) Configure NNM plugin import schedules, as described in [Edit Plugin and Feed Settings and Schedules](#). By default, Tenable.sc checks for new passive vulnerability plugins every 24 hours and pushes them to your attached NNM instances.

What to do next:

- View vulnerability data filtered by your NNM repository, as described in [Vulnerability Analysis](#).

Considerations for Licensing

If you want Tenable.sc to push plugin updates to NNM, you must add the product activation code to Tenable.sc. For more information, see [Apply a New License](#).



For detailed information about plugins counted toward the Tenable.sc license count, see [License Requirements](#).

Considerations for NNM Discovery Mode

Your NNM instances can run in two modes: discovery mode disabled and discovery mode enabled. For more information, see [NNM Settings](#) in the *Nessus Network Monitor User Guide*.

If discovery mode is enabled on an NNM instance, Tenable.sc stores discovery mode asset data to Tenable.sc repositories. Since discovery mode only discovers limited asset data, the repository data appears incomplete.

Tenable.sc does not count IP addresses present only from NNM instances in discovery mode toward your license count.



Add an NNM Instance

Required User Role: Administrator

Before you begin:

- Confirm you understand the complete scanning configuration process, as described in [Nessus Network Monitor Instances](#).

To add an NNM instance to Tenable.sc:

1. Log in to Tenable.sc via the user interface.
2. Click **Resources > Nessus Network Monitors**.

The **Nessus Network Monitor Scanners** page appears.

3. Click **Add**.

The **Add Nessus Network Monitor Scanner** page appears.

4. Configure the settings, as described in [NNM Instance Settings](#).
 - a. In the **Name** box, type a name for the scanner.
 - b. In the **Description** box, type a description for the scanner.
 - c. In the **Host** box, type the hostname or IP address for the scanner.
 - d. In the **Port** box, view the default (**8835**) and modify, if necessary.
 - e. If you want to disable this scanner's connection to Tenable.sc, click **Enabled** to disable the connection.
 - f. 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 NNM server, click **Verify Hostname** to enable the toggle.
 - g. If you want to use the proxy configured in NNM for communication with the scanner, click **Use Proxy** to enable the toggle.
 - h. In the **Type** drop-down box, select the authentication type.



- i. If you selected **Password** as the **Type**:
 - i. In the **Username** box, type the username for the account generated during the NNM installation for daemon-to-client client communications.
 - ii. In the **Password** box, type the password for the account generated during the NNM installation for daemon-to-client client communications
- j. If you selected **SSL Certificate** as the **Type**:
 - i. Click **Choose File** to upload a certificate.
 - 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.
- k. In the **Repositories** list, select one or more repositories where you want Tenable.sc to store the scanner data.

5. Click **Submit**.

Tenable.sc saves your configuration.



View Your NNM Instances

Required User Role: Administrator

For more information, see [Nessus Network Monitor Instances](#).

To view your NNM instances in Tenable.sc:

1. Log in to Tenable.sc via the user interface.
2. Click **Resources** > **Nessus Network Monitors**.

The **Nessus Network Monitor Scanners** page appears.

3. View details about each NNM instance.
 - **Name** — The name for the instance.
 - **Status** — The status of the instance.
 - **Host** — The IP address of the instance.
 - **Version** — The instance's NNM version.
 - **Uptime** — The length of time, in days, that the instance has been running.
 - **Last Report** — The date and time NNM most recently reported data to Tenable.sc.
4. (Optional) To manually refresh the **Status** data, in the **Options** drop-down box, click **Update Status**.

Tenable.sc refreshes the **Status** data.



NNM Instance Settings

Use the following options to configure NNM instances in Tenable.sc, as described in [Add an NNM Instance](#).

Option	Description
Name	Descriptive name for the NNM instance.
Description	Instance description, location, or purpose.
Host	Hostname or IP address of the instance.
Port	TCP port that the NNM instance listens on for communications from Tenable.sc. The default is port 8835.
State	A instance may be marked as Enabled or Disabled within Tenable.sc to allow or prevent access to the instance.
Authentication Type	Select Password or SSL Certificate for the authentication type to connect to the NNM instance.
Username	Username generated during the NNM install for daemon to client communications. This must be an administrator user in order to send plugin updates to the NNM instance. 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	This option is available if the Authentication Type is SSL Certificate . Click the Browse button, choose a SSL Certificate file to upload, and upload to the Tenable.sc.
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.
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 cer-



Option	Description
	tificate from the NNM server.
Use Proxy	Instructs Tenable.sc to use its configured proxy for communication with the instance.
Repositories	The repositories which this NNM instance will save its data to. If NNM will be reporting IPv4 and IPv6 data, at least two repositories (one for IPv4 and one for IPv6 data) must be selected.



Log Correlation Engines

Tenable Log Correlation Engine (LCE) is a software module that aggregates, normalizes, correlates, and analyzes event log data from the myriad of devices within the infrastructure. LCE also has the ability to analyze logs for vulnerabilities.

Tenable.sc performs vulnerability, compliance, and event management, but without LCE integration it does not directly receive logs or IDS/IPS events. With LCE integration, LCE processes the events and passes the results to Tenable.sc.

LCE's close integration with Tenable.sc allows you to centralize log analysis and vulnerability management for a complete view of your organization's security posture.

Note: If you add an LCE server to Tenable.sc and enable **Import Vulnerabilities**, LCE data counts against your Tenable.sc license. For more information, see [License Requirements](#).

For more information, see [Add a Log Correlation Engine Server](#).

If remote root or root equivalent user login is prohibited in your environment, you can add the LCE server using SSH key authentication. For more information, see [Manual LCE Key Exchange](#).

For information about Tenable.sc-Log Correlation Engine communications encryption, see [Encryption Strength](#).

Log Correlation Engine Options

Option	Description
Name	Name for the integrated Log Correlation Engine.
Description	Descriptive text for the integrated Log Correlation Engine.
Host	IP address of the integrated Log Correlation Engine.
Check Authentication	Whether Tenable.sc checks the status of authentication between itself and the LCE server.
Organizations	Organizations that can access data from the integrated Log Correlation Engine.
Repositories	The repositories where you want Tenable.sc to store the imported LCE



Option	Description
	data.
Port	The port where the LCE reporter is listening on the LCE server.
Username and Password	The username and password you want Tenable.sc to use for authentication to the LCE server to retrieve vulnerability information. This user account must be able to make changes on the remote system to enable the SSH key exchange between Tenable.sc and LCE. The appropriate permissions level is typically root, root equivalent, or other high-level user permissions on the LCE system. Tenable.sc uses these credentials a single time to exchange SSH keys for secure communication between Tenable.sc and LCE.



Add a Log Correlation Engine Server

Required User Role: Administrator

Tip: You can configure more than one Log Correlation Engine to work with Tenable.sc.

Before you begin:

- Confirm you understand the complete scanning configuration process, as described in [Log Correlation Engines](#).

To add an LCE server to Tenable.sc:

1. Log in to Tenable.sc via the user interface.
2. Click **Resources > Log Correlation Engines**.

The **LCE Servers** page appears.

3. Click **Add**.

The **Add LCE Server** window appears.

4. Configure the **General** options, as described in [Log Correlation Engines](#).
 - a. In the **Name** box, type a name for the LCE server.
 - b. In the **Description** box, type a description for the LCE server.
 - c. In the **Host** box, type the hostname or IP address for the LCE server.
 - d. In the **Port** box, view the default (**1243**) and modify, if necessary.
5. (Optional) To allow Tenable.sc to log in to the LCE server and retrieve vulnerability information:
 - a. Enable **Import Vulnerabilities**.

Note: If you use an LCE server with Tenable.sc, Tenable.sc counts the IP addresses associated with each imported instance against your license. For more information, see [License Requirements](#).



- b. Select a **Repository** for the event vulnerability data.
- c. Type a **Username** and **Password** you want Tenable.sc to use for access to the LCE server.

6. Click **Submit**.

Tenable.sc saves your configuration.

7. (Optional) If you enabled the **Check Authentication** option above, Tenable.sc checks its ability to authenticate with the LCE server.

- If authentication is successful, Tenable.sc displays a message to acknowledge that fact.
- If authentication fails, Tenable.sc prompts you for credentials to the LCE server:

- a. Type a username and password.
- b. Click **Push Key** to initiate the transfer of the SSH Key.

If the transfer is successful, Tenable.sc displays a message to acknowledge that fact.



Log Correlation Engine Clients

The LCE server manages configuration files for LCE 5.x clients remotely from the command line. Tenable.sc manages the configuration files for LCE 5.x clients via a graphical interface.

The default view for the LCE Clients page displays all of the available clients for the selected LCE server in the **Filters** section, and may be changed by updating the LCE Server filter. Use the other filter options, to narrow down the displayed clients for the selected server by a mix of criteria based on combinations of the displayed columns.

Current LCE Client versions display information in the table including their name, host address, authorization status, client type, host OS, assigned policy file, date last updated, and client version. LCE Client configurations can be managed from Tenable.sc.

Tip: Configured clients prior to version 5.x appear in the list without OS and policy information. However, these clients cannot have their policy files centrally managed from Tenable.sc.

Each client may have a name assigned to it to help easily identify the client. The currently assigned name appears in the **Name** column. To change the name, click on the client to edit from the list, and type the name. Client names may not contain spaces. Click the **Submit** button to save the change.

LCE Clients are initially configured to send their data to a particular LCE server, but must be authorized by the LCE sever for the server to accept the data. The client's authorization status appears in the left-side column. If there is no icon, the client is authorized to send data to the LCE server. If there is a broken link icon, the client is not authorized to send data to the LCE server. Toggle this by selecting the  menu for the client and clicking either the **Authorize** or **Revoke Authorization** from the list as appropriate.

Each client must have a policy assigned to it that specifies the appropriate data to send. The currently assigned policy appears in the **Policy** column. To change the assigned policy, select the client to edit and click the appropriate policy from the drop-down box. Search client policies by name by entering text into the Policy box. Click the **Submit** button to save the change. The policy updates on the client on its next connection.



Log Correlation Engine Client Policies

The **LCE Client Policies** page contains a list of all the client policies currently available for use by LCEclients. The list contains the name of the policy, the operating system it is configured for use on, and the type of client the policy can be applied to.

Example policy files are available for use with the names default and beginning with **TNS-**. You can use these policy files as is or export them to be used as a basis for custom policy files. Tenable may update or change these example policy files without notice, so using them as is may return different results at a later time.

Use the **Add** button to add customized LCEClient policy files to the LCE server and make them available for use. The **Name** option is appended to the beginning of the file name and offers a description of the function or use of the policy file. The **OS Type** is used in the file name to easily identify the OS for which the policy is designed. The **Client Type** indicates the LCE Client for which the policy is written. The **Source** option is used to select and upload the custom policy file or type the policy file into the box. Click the **Submit** button to save the policy file and send it to the LCE server.

Note: The default and **TNS** prefixes should only be used by policies supplied by Tenable. If you use default or **TNS** as a prefix for custom policy files, they may be overwritten or manipulated.

Select a policy, click the gear button drop-down menu, then click **Export** to save the policy to a local drive. The file is in XML format, which you can edit with standard text or XML editors.

Select a policy, click the gear button drop-down menu, then click **View** to display the policy name and source of the policy in a window within Tenable.sc. You cannot edit the information from within this window.

Note: For more information on creating LCE Client policy files, see the *LCE Client Guide*.



Tenable.ot Instances

Tenable.ot protects industrial networks by providing industrial and critical infrastructure operations with visibility, security, and control to ensure safe facility operation while reducing overall risk. You can use Tenable.sc to analyze Tenable.ot asset and vulnerability data alongside your data from other scanners.

When you configure data synchronization from Tenable.ot to Tenable.sc, Tenable.ot sends asset and vulnerability data to an agent repository in Tenable.sc. Tenable.ot communicates with Tenable.sc using the Tenable.sc API.

Note: It is important to restrict the data Tenable.ot collects to only the desired host IP address ranges. For example, if Tenable.ot collects information on 1100 hosts and Tenable.sc is licensed for 1000 hosts, Tenable.ot sends all of the data to Tenable.sc and Tenable.sc will indicate that you exceeded your host count. For more information, see [License Requirements](#).

Before you begin:

- Deploy Tenable.ot, as described in the *Tenable.ot User Guide*.
- Begin vulnerability assessment in Tenable.ot, as described in the *Tenable.ot User Guide*.

To fully configure data synchronization from Tenable.ot to Tenable.sc:

1. Add a designated agent repository for Tenable.ot data in Tenable.sc, as described in [Add a Repository](#).
2. Using the Tenable.ot API, configure the Tenable.sc integration to specify the sync schedule, import repository, and authentication.

What to do next:

- View scan results from Tenable.ot, as described in [View Scan Results](#).
- View vulnerability data filtered by your Tenable.ot repository, as described in [Vulnerability Analysis](#).



Repositories

Repositories are databases within Tenable.sc that contain vulnerability data. You can share repositories with users and organizations based on admin-defined assets. Repositories provide scalable and configurable data storage. Optionally, you can share repository data between multiple Tenable.sc's.

Note: The maximum repository size is 32 GB.

When adding a *local repository*, you designate storage within Tenable.sc for different types of vulnerability data (identified by IPv4 addresses, IPv6 addresses, agents, or mobile scanners). Scanners attached to a Tenable.sc populate your local repositories with vulnerability data. For more information, see [Local Repositories](#).

When adding an *external repository*, you access a local repository from another Tenable.sc:

- Remote repositories allow you to share repository data from one Tenable.sc deployment to your primary Tenable.sc deployment via an SSH session.
- Offline repositories allow you to share repository data from one Tenable.sc deployment to your primary Tenable.sc deployment via manual export and import (a `.tar.gz` archive file). You can combine data from several repository files into a single offline repository by importing multiple files to the offline repository.

External repository data is static and used solely for reporting purposes. For more information, see [External Repositories](#).

For more information, see [Add a Repository](#) and [Manage Repositories](#). For information about Tenable.sc 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.



Add a Repository

Required User Role: Administrator

For more information about repositories, see [Repositories](#).

Before you begin:

- If you are adding a remote or offline repository, confirm that your other Tenable.sc is running version 5.0.0 or later.

Note: If you want to configure an agent repository as a remote or offline repository, you must upgrade both Tenable.sc deployments to version 5.7.1 or later.

To add a repository:

1. Log in to Tenable.sc via the user interface.
2. Click **Repositories > Repositories**.

The Repositories page appears.

3. 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 type:

- [IPv4/IPv6 Repositories](#)
- [Mobile Repositories](#)
- [Agent Repositories](#)
- [Remote Repositories](#)
- [Offline Repositories](#)



6. Click **Submit**.

Tenable.sc saves your configuration.

What to do next:

- If you added an offline repository, export one or more repositories from your other Tenable.sc as described in [Export a Repository](#).
- If you added an offline repository, import one or more exported repository files as described in [Import a Repository](#).



Manage Repositories

Required User Role: Administrator

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

To manage your repositories:

1. Log in to Tenable.sc via the user interface.
2. Click **Repositories** > **Repositories**.

The **Repositories** page appears.

3. To filter the repositories that appear on the page, apply a filter as described in [Apply a Filter](#).
4. To view details for a repository:
 - a. In the row for the repository, click the  menu.

The actions menu appears.

- b. Click **View**.

The **View Repository** page appears. For more information, see [Repository Details](#).

5. To edit a repository:
 - a. In the row for the repository, click the  menu.

The actions menu appears.

- b. Click **Edit**.

The **Edit Repository** page appears.

- c. Modify the repository options, as described in [IPv4/IPv6 Repositories](#), [Mobile Repositories](#), [Agent Repositories](#), [Remote Repositories](#), or [Offline Repositories](#).
- d. Click **Submit**.

Tenable.sc saves your configuration.

6. To export a repository, see [Export a Repository](#).



7. To import a repository file into an offline repository, see [Import a Repository](#).
8. To delete a repository, see [Delete a Repository](#).



View Your Repositories

Required User Role: Administrator

You can view a list of all repositories on your Tenable.sc. For more information, see [Repositories](#).

To view a list of your repositories:

1. Log in to Tenable.sc via the user interface.
2. Click **Repositories** > **Repositories**.

The **Repositories** page appears.

3. 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.
- **Last Updated** — The date and time the repository was last updated.



View Repository Details

Required User Role: Administrator

You can view details for any repository. For more information, see [Repositories](#).

To view repository details:

1. Log in to Tenable.sc via the user interface.
2. Click **Repositories** > **Repositories**.

The **Repositories** page appears.

3. In the row for the repository, click the  menu.

The actions menu appears.

4. Click **View**.

The **View Repository** page appears.

Section	Repository Type	Action
General	All	View general information for the repository. • Name — The repository name. • Description — The repository description. • Created — The date the repository was created. • Last Modified — The date the repository was last modified. • ID — The repository ID.
MDM	Mobile	View a summary of your settings for the repository. For more information about a



Section	Repository Type	Action
		setting, see Mobile Repositories .
Data	IPv4/IPv6, Agent, Remote, Offline	View a summary of the repository data (for example, the IP address range). For more information, see: • IPv4/IPv6 Repositories • Agent Repositories • Remote Repositories • Offline Repositories
Access	All	View the name of the organizations with access to this repository.
Advanced Settings	IPv4/IPv6, Agent, Remote, Offline	View a summary of your settings for the repository. For more information about a setting, see: • IPv4/IPv6 Repositories • Agent Repositories • Remote Repositories • Offline Repositories
Tenable.io Synchronization Data	All supported for Lumin synchronization	View synchronization summary data: • Status – The status of the repository in Lumin synchronization: • Finished – The most recent synchronization that included this repository succeeded. • Not Synced – The repository is



Section	Repository Type	Action
		not configured for Lumin synchronization. • Error – An error occurred. For more information, see View Lumin Data Synchronization Logs. • First Synchronization – The date and time of the first synchronization of this repository. • Last Success – The date and time of the most recent synchronization of this repository. • Last Failure – The date and time of the most recent failed synchronization of this repository. For more information about Lumin synchronization, see Lumin Synchronization.



Export a Repository

Required User Role: Administrator

You can export a repository from one Tenable.sc and import it as an offline repository on another Tenable.sc. You can export repositories via the Tenable.sc 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.

Tip: If the repository you want to export has trend data enabled and you want to include trend data in your repository export, export the repository via the CLI. Repositories that you export via the user interface do not include trend data. For more information about trend data, see [IPv4/IPv6 Repositories](#) and [Agent Repositories](#).

To export a repository via the user interface:

1. Log in to Tenable.sc via the user interface.
2. Click **Repositories > Repositories**.

The **Repositories** page appears.

3. In the row for the repository, click the  menu.

The actions menu appears.

4. Click **Export**.

Tenable.sc exports the repository.

To export a repository via the CLI:

1. Log in to Tenable.sc via the command line interface (CLI).
2. Prepare the command you want to run.

```
/opt/sc/customer-tools/exportRepository.sh [repID] [trendingDays]  
[trendWithRaw]
```



Variable	Description
<i>repID</i>	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 Repository Details .
<i>trendingDays</i>	(IP and Agent 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 IPv4/IPv6 Repositories and Agent Repositories .
<i>trendWithRaw</i>	(IP and agent 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.sc, run the export command.

For example:

```
/opt/sc/customer-tools/exportRepository.sh 1 default default -f
```

Tenable.sc exports the repository.

What to do next:

- To import the repository to another Tenable.sc, add an offline repository to that Tenable.sc, as described in [Add a Repository](#).



Import a Repository

Required User Role: Administrator

You can import one or more repository files to an offline repository. For more information, see [Offline Repositories](#).

Note: When importing the repository archive, the default maximum file import size is 360MB. This is specified by the **post_max_size** directive in `/opt/sc/support/etc/php.ini`. If larger file uploads are required, increase the default value.

Before you begin:

- Export one or more repository files from your other Tenable.sc, as described in [Export a Repository](#).
- Add an offline repository, as described in [Add a Repository](#).

To import an exported repository to an offline repository:

1. Log in to Tenable.sc via the user interface.
2. Click **Repositories > Repositories**.

The **Repositories** page appears.

3. In the row for the offline repository you created, click the  menu.

The actions menu appears.

4. Click **Upload** and browse to the file you want to upload.

Tenable.sc imports the repository.



Delete a Repository

Required User Role: Administrator

To delete a repository:

1. Log in to Tenable.sc via the user interface.
2. Click **Repositories** > **Repositories**.

The **Repositories** page appears.

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

The actions menu appears.

4. Click **Delete**.

A confirmation window appears.

5. Click **Delete**.

Tenable.sc deletes the repository.



Local Repositories

When adding *local repositories*, you designate storage within Tenable.sc for different types of vulnerability data. Scanners attached to a Tenable.sc populate your local repositories with vulnerability data.

Tenable.sc supports three types of local repositories: [IPv4/IPv6 Repositories](#), [Mobile Repositories](#), and [Agent Repository Options](#).

For more information, see [Repositories](#) and [Add a Repository](#).



IPv4/IPv6 Repositories

These are the most common types of repositories used with Tenable.sc. They store IPv4 and IPv6 data from active and passive scans. Data stored in local repositories can be shared between organizations and includes the full range of event and vulnerability metadata.

Caution: When creating Tenable.sc IPv4 or IPv6 repositories, LCE event source IP address ranges must be included along with the vulnerability IP address ranges or the event data and event vulnerabilities are not accessible from the Tenable.sc web interface.

For more information, see [Add a Repository](#).

IP Repository Options

Option	Description
General	
Name	The repository name.
Description	(Optional) A description for the repository.
Data	
IP Ranges	Specifies the IP address range of vulnerability data you want to store in the repository. Type the range as a comma-delimited list of IP addresses, IP address ranges, and/or CIDR blocks.
Access	
Organizations	Specifies which organizations have access to the vulnerability data stored in the repository. If groups are configured for the organization, Tenable.sc prompts you to grant or deny access to all of the groups in the organization. For more granular control, grant access within the settings for that group.
Advanced Settings	



Option	Description
Generate Trend Data	When enabled, Tenable.sc generates trend data by taking periodic snapshots of the cumulative database. Trend data is displayed in some Tenable.sc tools (e.g., trending line charts and trending area charts). Tenable.sc also produces differential data (snapshot comparison data), which improves performance when displaying trend data in Tenable.sc tools. Tip: Disable this option to reduce your disk space usage.
Days Trending	Specifies the number of days of cumulative vulnerability data that you want Tenable.sc to display in dashboard and report vulnerability trending displays.
Enable Full Text Search	When enabled, Tenable.sc includes vulnerability text in periodic snapshots of .nessus data for vulnerability trending purposes. For more information about the Vulnerability Text filter component, see Vulnerability Analysis Filter Components.
LCE Correlation	Not supported for IPv6 repositories. The LCE server where you want Tenable.sc to retrieve data. The data retrieved depends on the Import Vulnerabilities setting in your LCE server configuration: • If Import Vulnerabilities is enabled, Tenable.sc retrieves vulnerability data and LCE events. • If Import Vulnerabilities is disabled, Tenable.sc retrieves LCE events.



Mobile Repositories

The mobile repository is a local type that stores data from various servers. For more information, see [Add a Repository](#).

- [General Options](#)
- [ActiveSync Options](#)
- [AirWatch MDM Options](#)
- [Apple Profile Manager Options](#)
- [Blackberry UEM Options](#)
- [Good MDM Options](#)
- [Microsoft Intune Options](#)
- [Mobile Iron Options](#)

General Options

Configure the following options for all mobile repository types.

Option	Description	Default
Name	The repository name.	--
Description	(Optional) A description for the repository.	--
Type	The type of repository you want to configure. Your Type selection determines the type-specific options you must configure: ActiveSync Options , AirWatch MDM Options , Apple Profile Manager Options , Blackberry UEM Options , Good MDM Options , Microsoft Intune Options , or Mobile Iron Options .	--
Organizations	Specifies which organizations have access to the vulnerability data stored in the repository. If groups are configured for the organization, Tenable.sc	--



Option	Description	Default
	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.	

ActiveSync Options

The following table describes the additional options to configure when creating an **ActiveSync** mobile repository.

Option	Description	Default
Domain Controller	(Required) The domain controller for ActiveSync.	--
Domain	(Required) The Windows domain for ActiveSync.	--
Domain Username	(Required) The username for the domain administrator's account that Tenable.sc uses to authenticate to ActiveSync.	--
Domain Password	(Required) The password for the domain administrator user.	--
Scanner	(Required) Specifies which Nessus scanner Tenable.sc uses when scanning the server. Tenable.sc can only use one Nessus scanner to add data to a mobile repository.	--
Update Schedule	Sets the schedule for the MDM server to be scanned to update the mobile repository. On each scan, the current data in the repository is removed and replaced with the information from the latest scan.	Every day at 12:30 - 04:00

AirWatch MDM Options

The following table describes the additional options to configure when creating an **AirWatch MDM** mobile repository.



Option	Description	Default
AirWatch Environment API URL	(Required) The SOAP URL or REST API URL you want Tenable.sc to use to authenticate with AirWatch.	--
Port	(Required) The TCP port that AirWatch listens on for communications from Tenable.sc.	443
Username	(Required) The username for the AirWatch user account Tenable.sc uses to authenticate to AirWatch's REST API.	--
Password	(Required) The password for the AirWatch user.	--
API Key	(Required) The API key for the AirWatch REST API.	--
HTTPS	When enabled, Tenable.sc connects using secure communication (HTTPS). When disabled, Tenable.sc connects using standard HTTP.	Enabled
Verify SSL Certificate	When enabled, Tenable.sc verifies that the SSL certificate on the server is signed by a trusted CA. Tip: If you are using a self-signed certificate, disable this setting.	Enabled
Scanner	(Required) Specifies which Nessus scanner Tenable.sc uses when scanning the server. Tenable.sc can only use one Nessus scanner to add data to a mobile repository.	--
Update Schedule	Specifies when Tenable.sc scans the server to update the mobile repository. On each scan, Tenable.sc removes the current data in the repository and replaces it with data from the latest scan.	Every day at 12:30 - 04:00

Apple Profile Manager Options

The following table describes the additional options to configure when creating an **Apple Profile Manager** mobile repository.



Option	Description	Default
Server	(Required) The server URL Tenable.sc uses to authenticate with Apple Profile Manager.	--
Port	(Required) The TCP port that Apple Profile Manager listens on for communications from Tenable.sc.	443
Username	The username for the Apple Profile Manager user account Tenable.sc uses to authenticate to Apple Profile Manager.	--
Password	The password for the Apple Profile Manager user.	--
HTTPS	When enabled, Tenable.sc connects using secure communication (HTTPS). When disabled, Tenable.sc connects using standard HTTP.	Enabled
Verify SSL Certificate	When enabled, Tenable.sc verifies that the SSL certificate on the server is signed by a trusted CA. Tip: If you are using a self-signed certificate, disable this setting.	Enabled
Scanner	(Required) Specifies which Nessus scanner Tenable.sc uses when scanning the server. Tenable.sc can only use one Nessus scanner to add data to a mobile repository.	--
Update Schedule	Specifies when Tenable.sc scans the server to update the mobile repository. On each scan, Tenable.sc removes the current data in the repository and replaces it with data from the latest scan.	Every day at 12:30 - 04:00

Blackberry UEM Options

The following table describes the additional options to configure when creating a **Blackberry UEM** mobile repository.



Option	Description	Default
Blackberry UEM Hostname	(Required) The hostname for the Blackberry UEM server.	--
Blackberry UEM Port	(Required) The port you want Tenable.sc to use for authenticating to the Blackberry UEM server.	--
Blackberry UEM Tenant	(Required) The SRP ID value in Blackberry UEM.	--
Blackberry UEM Domain	The domain name value in Blackberry UEM.	--
Blackberry UEM Username	(Required) The username for the Blackberry UEM user account Tenable.sc uses to authenticate to Blackberry UEM.	--
Blackberry UEM Password	(Required) The password for the Blackberry UEM user.	--
Blackberry UEM SSL	When enabled, Tenable.sc uses an encrypted connection to authenticate with Blackberry UEM.	Disabled
Blackberry UEM Verify SSL Certificate	When enabled, Tenable.sc verifies that the SSL certificate on the server is signed by a trusted CA. Tip: If you are using a self-signed certificate, disable this setting.	Disabled
Scanner	(Required) Specifies which Nessus scanner Tenable.sc uses when scanning the server. Tenable.sc can only use one Nessus scanner to add data to a mobile repository.	--
Update Schedule	Specifies when Tenable.sc scans the server to update the mobile repository. On each scan, Tenable.sc removes the current data in the repository and replaces it with data from the latest scan.	Every day at 12:30 - 04:00

Good MDM Options



The following table describes the additional options to configure when creating a **Good MDM** mobile repository.

Option	Description	Default
Server	(Required) The server URL Tenable.sc uses to authenticate with Good MDM.	--
Port	(Required) The TCP port that Good MDM listens on for communications from Tenable.sc.	--
Domain	(Required) The domain name for Good MDM.	--
Username	(Required) The username for the Good MDM user account Tenable.sc uses to authenticate to Good MDM.	--
Password	(Required) The password for the Good MDM user.	--
HTTPS	When enabled, Tenable.sc connects using secure communication (HTTPS). When disabled, Tenable.sc connects using standard HTTP.	Enabled
Verify SSL Certificate	When enabled, Tenable.sc verifies that the SSL certificate on the server is signed by a trusted CA. Tip: If you are using a self-signed certificate, disable this setting.	Enabled
Scanner	(Required) Specifies which Nessus scanner Tenable.sc uses when scanning the server. Tenable.sc can only use one Nessus scanner to add data to a mobile repository.	--
Update Schedule	Specifies when Tenable.sc scans the server to update the mobile repository. On each scan, Tenable.sc removes the current data in the repository and replaces it with data from the latest scan.	Every day at 12:30 - 04:00

Microsoft Intune Options



The following table describes the additional options to configure when creating a **Microsoft Intune** mobile repository.

Option	Description	Default
Intune Tenant	(Required) The Microsoft Azure Directory value in your Microsoft Intune registration.	--
Intune Client	(Required) The Microsoft Azure Application value generated during your Microsoft Intune registration.	--
Intune Secret	(Required) The Microsoft Azure client secret key.	--
Intune Username	(Required) The username for the Microsoft Intune user account Tenable.sc uses to authenticate to Microsoft Intune.	--
Intune Password	(Required) The password for the Microsoft Intune user.	--
Scanner	(Required) Specifies which Nessus scanner Tenable.sc uses when scanning the server. Tenable.sc can only use one Nessus scanner to add data to a mobile repository.	--
Update Schedule	Specifies when Tenable.sc scans the server to update the mobile repository. On each scan, Tenable.sc removes the current data in the repository and replaces it with data from the latest scan.	Every day at 12:30 - 04:00

Mobile Iron Options

The following table describes the additional options to configure when creating a **Mobile Iron** mobile repository.

Option	Description	Default
MobileIron VSP Admin Portal URL	(Required) The server URL Tenable.sc uses to authenticate to the MobileIron administrator portal.	--
VSP Admin Portal Port	The TCP port that the MobileIron administrator portail listens on for communications from Tenable.sc.	--



Option	Description	Default
MobileIron Port	(Required) The TCP port that MobileIron listens on for communications from Tenable.sc.	443
Username	(Required) The username for the MobileIron administrator account Tenable.sc uses to authenticate to MobileIron.	--
Password	(Required) The password for the MobileIron administrator user.	--
HTTPS	When enabled, Tenable.sc connects using secure communication (HTTPS). When disabled, Tenable.sc connects using standard HTTP.	Enabled
Verify SSL Certificate	When enabled, Tenable.sc verifies that the SSL certificate on the server is signed by a trusted CA. Tip: If you are using a self-signed certificate, disable this setting.	Enabled
Scanner	(Required) Specifies which Nessus scanner Tenable.sc uses when scanning the server. Tenable.sc can only use one Nessus scanner to add data to a mobile repository.	--
Update Schedule	Specifies when Tenable.sc scans the server to update the mobile repository. On each scan, Tenable.sc removes the current data in the repository and replaces it with data from the latest scan.	Every day at 12:30 - 04:00



Agent Repositories

Agent repositories can store data from Nessus Agents (identified by agent ID) or Tenable.ot (identified by Tenable.ot UUID).

An agent ID uniquely identifies agent-detected assets that may share a common IP address.

Tenable.ot assigns UUIDs to assets in order to uniquely identify them, since not all operational technology assets have IP addresses. Then, Tenable.sc uses the UUIDs to uniquely identify Tenable.ot data in Tenable.sc. For more information about viewing Tenable.ot data in Tenable.sc, see [Tenable.ot Instances](#).

For more information, see [Add a Repository](#).

Agent Repository Options

Option	Description
General	
Name	The repository name.
Description	(Optional) A description for the repository.
Access	
Organizations	Specifies which organizations have access to the vulnerability data stored in the repository. If groups are configured for the organization, Tenable.sc prompts you to grant or deny access to all of the groups in the organization. For more granular control, grant access within the settings for that group.
Advanced Settings	
Generate Trend Data	When enabled, Tenable.sc generates trend data by taking periodic snapshots of the cumulative database. Trend data is displayed in some Tenable.sc tools (e.g., trending line charts and trending area charts). Tenable.sc also produces differential data (snapshot comparison data), which improves performance when displaying trend data in Tenable.sc



Option	Description
	tools. Tip: Disable this option to reduce your disk space usage.
Days Trending	Specifies the number of days of cumulative vulnerability data that you want Tenable.sc to display in dashboard and report vulnerability trending displays.
Enable Full Text Search	When enabled, Tenable.sc includes vulnerability text in periodic snapshots of .nessus data for vulnerability trending purposes. For more information about the Vulnerability Text filter component, see Vulnerability Analysis Filter Components .



External Repositories

When adding an *external repository*, you access a local repository from another Tenable.sc:

- Offline repositories allow you to share repository data from one Tenable.sc deployment to your primary Tenable.sc deployment via manual export and import (a `.tar.gz` archive file). You can combine data from several repository files into a single offline repository by importing multiple files to the offline repository.
- Remote repositories allow you to share repository data from one Tenable.sc deployment to your primary Tenable.sc deployment via an SSH session.

External repository data is static and used solely for reporting purposes. For more information, see [Offline Repository Options](#) and [Remote Repositories](#).

For more information, see [Repositories](#) and [Add a Repository](#).



Offline Repositories

Offline repositories allow you to share repository data from one Tenable.sc deployment to your primary Tenable.sc deployment via manual export and import (a `.tar.gz` archive file). You can combine data from several repository files into a single offline repository by importing multiple files to the offline repository.

Offline repositories are particularly useful to export data from air-gapped instances of Tenable.sc. For more information, see [Considerations for Air-Gapped Environments](#).

Note: You must upgrade both Tenable.sc deployments to version 5.7.1 or later in order to configure agent repositories as offline repositories.

Note: You cannot set an offline repository as the **Import Repository** for active scans. You can only use offline repository data for reporting purposes.

To fully configure an offline repository:

1. [Add an offline repository](#) to your primary Tenable.sc deployment.
2. [Export](#) one or more repositories from your other Tenable.sc deployment.
3. [Import](#) one or more repositories to the offline repository on your primary Tenable.sc deployment.

Offline Repository Options

Option	Description
General	
Name	The repository name.
Description	(Optional) A description for the repository.
Access	
Data Type	The type of data in the other Tenable.sc repository: IPv4 , IPv6 , Mobile , or Agent .
IP Ranges	If the Data Type is IPv4 or IPv6 , specifies the IP address range of vul-



Option	Description
	nerability data that you want to view in the offline repository. For example, to view all data from the exported repository file, specify a range that includes all data in that repository. Type the range as a comma-delimited list of IP addresses, IP address ranges, and/or CIDR blocks. For more information, see IPv4/IPv6 Repositories.
Type	If the Data Type is Mobile, the type of mobile repository: ActiveSync, AirWatch MDM, Apple Profile Manager, Blackberry UEM, Good MDM, Microsoft Intune, or Mobile Iron. For more information, see Mobile Repositories.
Access	
Organizations	Specifies which organizations have access to the vulnerability data stored in the repository. If groups are configured for the organization, Tenable.sc prompts you to grant or deny access to all of the groups in the organization. For more granular control, grant access within the settings for that group.
Advanced Settings	
Generate Trend Data	When enabled, Tenable.sc generates trend data by taking periodic snapshots of the cumulative database. Trend data is displayed in some Tenable.sc tools (e.g., trending line charts and trending area charts). Tenable.sc also produces differential data (snapshot comparison data), which improves performance when displaying trend data in Tenable.sc tools. Tip: Disable this option to reduce your disk space usage.
Days Trending	Specifies the number of days of cumulative vulnerability data that you want Tenable.sc to display in dashboard and report vulnerability trending



Option	Description
	displays.
Enable Full Text Search	When enabled, Tenable.sc includes vulnerability text in periodic snapshots of .nessus data for vulnerability trending purposes. For more information about the Vulnerability Text filter component, see Vulnerability Analysis Filter Components .



Remote Repositories

Remote repositories allow you to share repository data from one Tenable.sc deployment to your primary Tenable.sc deployment via an SSH session.

Note: You cannot set a remote repository as the **Import Repository** for active scans. You can use remote repository data only for reporting purposes.

For more information, see [Add a Repository](#).

To use tiered remote repositories for large enterprise deployments of Tenable.sc, see [Tiered Remote Repositories](#).

Option	Description
General	
Name	The repository name.
Description	(Optional) A description for the repository.
Remote Tenable.sc	
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.sc. The Tenable.sc deployments exchange SSH keys, and the system populates the Repository list with all available repositories from the remote Tenable.sc.
Repository	The remote repository you want to collect IP addresses and vulnerability data from.
Update Schedule	Sets the schedule for the remote server to be queried for updated information.



Option	Description
Access	
Organizations	Specifies which organizations have access to the vulnerability data stored in the repository. If groups are configured for the organization, Tenable.sc prompts you to grant or deny access to all of the groups in the organization. For more granular control, grant access within the settings for that group.



Tiered Remote Repositories

Remote repositories allow you to share repository data from one Tenable.sc deployment to your primary Tenable.sc deployment via an SSH session.

A *tiered remote repository* configuration uses remote repositories to share data between multiple Tenable.sc instances.

- If you plan to support 100,000–249,999 hosts, Tenable recommends a tiered remote repository configuration.
- If you plan to support 250,000 or more hosts, Tenable **requires** a tiered remote repository configuration.

Tiered Tenable.sc instances perform informal roles in your overall Tenable.sc deployment. Tenable recommends at least one designated reporting Tenable.sc and an additional Tenable.sc instance for every 100,000 to 150,000 hosts on your network.

- A *scanning tier* Tenable.sc optimizes scanning by managing scan jobs across your attached scanners. Scanning tier Tenable.sc instances prioritize efficient collection of scan data.
- A *reporting tier* Tenable.sc optimizes dashboards and reporting by centralizing the data collected by scanning tier Tenable.sc instances.

Note: Your scanning tier and reporting tier Tenable.sc instances must be running the same Tenable.sc version.

Without a tiered remote repository configuration, enterprise-scale scanning and analysis may cause performance issues on a single Tenable.sc. Tiered remote repositories optimize your analysis and report generation without negatively impacting scanning performance.

For more information, see [Configure Tiered Remote Repositories](#).

Tip: Configuring tiered remote repositories does not allow you to monitor the status of scanning tier Tenable.sc instances. To monitor the status of multiple Tenable.sc instances, connect your Tenable.sc instances to Tenable.sc Director. For more information about Tenable.sc Director, see the *Tenable.sc Director User Guide*.



Configure Tiered Remote Repositories

You may want to configure tiered remote repositories in large deployments of Tenable.sc. For more information, see [Tiered Remote Repositories](#).

To configure a tiered remote repository deployment:

1. On the scanning tier Tenable.sc instance, [create one or more repositories](#) for storing scan result data.

Note: To view trend data for scanning tier Tenable.sc instances on your reporting tier Tenable.sc instance, enable the **Generate Trend Data** option for each repository on your scanning tier Tenable.sc instances. For more information, see [Agent Repositories](#) and [IPv4/IPv6 Repositories](#).

2. On the scanning tier Tenable.sc instance, [run scans](#) to populate the repositories with data.
3. On the reporting tier Tenable.sc instance, [create a remote repository](#) for each repository on your scanning tier Tenable.sc instance.

The reporting tier Tenable.sc syncs scan result data from the scanning tier Tenable.sc repositories.



Active Scans

In active scanning, the scanner sends packets to a remote target to provide a snapshot of network services and applications. These are compared to a plugin database to determine if any vulnerabilities are present. Tenable.sc can also use a scanner located outside the local network to simulate what an external entity might see.

For more information about supported active scanner types (Nessus and Tenable.io deployments) in Tenable.sc, see [Nessus Scanners](#).

Credentialed Nessus scans, a type of active scanning, can be leveraged to perform highly accurate and rapid patch, configuration, and vulnerability audits on Unix, Windows, Cisco, and database systems by actually logging in to the target system with provided credentials. Credentialed scans can also enable the ability to enumerate all UDP and TCP ports in just a few seconds. Tenable.sc can securely manage these credentials across thousands of different systems and also share the results of these audits only with users who have a need to know.

For more information, see [Manage Active Scans](#) and [Active Scan Settings](#).

To fully configure active scans using a Nessus or Tenable.io scanner:

1. If you are configuring a Nessus scanner (not a Tenable.io deployment), configure scanning in Nessus, as described in [Scans](#) in the *Nessus User Guide*.

Note: For information about credentialed scanning in Nessus, see [Credentialed Checks](#) in the *Nessus User Guide*.

2. Add the Nessus scanner or your Tenable.io deployment in Tenable.sc, as described in [Nessus Scanners](#).
3. Add a scan zone in Tenable.sc, as described in [Add a Scan Zone](#).
4. Add a repository for the scan data in Tenable.sc, as described in [Add a Repository](#).
5. Create active scan objects in Tenable.sc, as described in:
 - a. [Add a Template-Based Asset](#) or [Add a Custom Asset](#).
 - b. [Add Credentials](#).



- c. [Add a Template-Based Audit File](#) or [Add a Custom Audit File](#).
- d. [Add a Scan Zone](#).
- e. [Add a Scan Policy](#).

6. Add an active scan in Tenable.sc, as described in [Add an Active Scan](#).

What to do next:

- View scan results, as described in [Scan Results](#).
- View vulnerability data by IP address, as described in [Vulnerability Analysis](#).

Special Active Scans

Diagnostic Scans

If you experience issues with an active scan, Tenable Support may ask you to run a diagnostic scan to assist with troubleshooting. After Tenable.sc runs the diagnostic scan, download the diagnostic file and send it to Tenable Support.

For more information, see [Run a Diagnostic Scan](#).

Remediation Scans

You can run a remediation scan to run a followup active scan against existing active scan results. A remediation scan evaluates a specific plugin against a specific target or targets where the related vulnerability was present in your earlier active scan.

For more information, see [Launch a Remediation Scan](#).



Add an Active Scan

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

For more information about active scan options, see [Active Scan Settings](#).

Before you begin:

- Confirm you are running Nessus 6.3.6 or later.
- Confirm you understand the complete scanning configuration process, as described in [Active Scans](#).

To add an active scan:

1. Log in to Tenable.sc via the user interface.
2. Click **Scans > Active Scans**.
The **Active Scans** page appears.
3. Click **Add**.
The **Add Active Scan** page appears.
4. Click **General**.
5. Type a **Name** for the scan.
6. (Optional) Type a **Description** for the scan.
7. Select a **Policy** for the scan.
8. (Optional) If you want to schedule the scan to run automatically, select a **Schedule** for the scan.
9. Click **Settings**.
10. If prompted, select a preconfigured **Scan Zone** for the scan.
11. Select an **Import Repository** for the scan.
12. Select a **Scan Timeout Action** for the scan.
13. Select a **Rollover Schedule** for the scan.



14. Enable or disable the **Advanced** options.
15. Click **Targets**.
16. The page updates to show the required options for that target type.
17. Select a **Target Type** for the scan.
18. Select one or more **Assets** and/or **IPs / DNS Names** for the scan.
19. (Optional) In the **Credentials** section, if you want to configure credentialed scanning, click **Add Credential**. Then:
 - a. In the drop-down boxes, select a credential type and a preconfigured credential.
 - b. Click the check mark to save your selection.
20. (Optional) If you want to configure multiple credentials for the active scan, repeat step 19.

Note: When running an active scan, Tenable.sc attempts authentication using the newest credentials added by an Administrator user. If the newest Administrator-added credentials do not match, Tenable.sc attempts authentication with older Administrator-added credentials.

Then, if no Administrator-added credentials match, Tenable.sc attempts to authenticate using the newest credentials added by an organizational user. If the newest organizational user-added credentials do not match, Tenable.sc attempts authentication with older organizational user-added credentials.

If no credentials match, the scan runs without credentialed access.

21. In the **Post Scan** section:
 - a. (Optional) If you previously added an email address to your account profile and you want to configure email notifications, enable or disable **E-Mail Me on Launch** or **E-Mail Me on Completion**.
 - b. (Optional) If you want to configure automatic report generation, click **Add Report**. For more information, see [Add a Report to a Scan](#).
22. Click **Submit**.

Tenable.sc saves your configuration.



Manage Active Scans

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

For more information about active scans, see [Active Scans](#).

To manage active scans:

1. Log in to Tenable.sc via the user interface.
2. Click **Scans > Active Scans**.

The **Active Scans** page appears.

3. To filter the scans that appear on the page, apply a filter as described in [Apply a Filter](#).
4. To start or pause a scan, see [Start or Pause a Scan](#).
5. To suspend or resume a scheduled scan, see [Suspend or Resume a Scheduled Active Scan](#).

6. To view details for a scan:

- a. In the row for the scan, click the  menu.

The actions menu appears.

- b. Click **View**.

The **View Active Scan** page appears.

7. To edit a scan:

- a. In the row for the scan, click the  menu.

The actions menu appears.

- b. Click **Edit**.

The **Edit Active Scan** page appears.

- c. Modify the scan options.

- d. Click **Submit**.



Tenable.sc saves your configuration.

8. To copy a scan:

- a. In the row for the scan, click the  menu.

The actions menu appears.

- b. Click **Copy**.

Tenable.sc creates a copy of the scan.

9. To run a diagnostic scan, see [Run a Diagnostic Scan](#).

10. To delete a scan:

- a. In the row for the scan, click the  menu.

The actions menu appears.

- b. Click **Delete**.

A confirmation window appears.

- c. Click **Delete**.

Tenable.sc deletes the scan.



Start or Pause a Scan

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

To start or pause an active scan, agent scan, or agent synchronization job:

1. Log in to Tenable.sc.
2. Click one of the following:
 - **Scans > Active Scans** (to manage active scans)
 - **Scans > Agent Synchronization Jobs** (to manage agent synchronization jobs)
 - **Scans > Agent Scans** (to manage agent scans)
 - **Scans > Scan Results** (to manage a scan from the results page).
3. Do one of the following:
 - To pause the scan or synchronization job, click the pause button on the right side of the scan or synchronization job row.
 - To start the scan or synchronization job, click the start button on the right side of the scan or synchronization job row.



Suspend or Resume a Scheduled Active Scan

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

If you suspend a scheduled active scan, Tenable.sc stops launching new scans for that active scan configuration. Tenable.sc does not disrupt scans already in progress or prevent users from launching scans on demand.

If you resume a suspended active scan, Tenable.sc resumes launching scans on the schedule configured for that active scan.

For more information, see [Active Scans](#).

Before you begin:

- Configure a scheduled active scan, as described in [Add an Active Scan](#).

To suspend or resume a scheduled active scan:

1. Log in to Tenable.sc via the user interface.
2. Click **Scans > Active Scans**.

The **Active Scans** page appears.

3. In the row for the scheduled scan you want to suspend or resume, click the  menu.

The actions menu appears.

4. Click **Suspend Schedule** or **Resume Schedule**.

The page updates to reflect the scan schedule status. When a scan is suspended, Tenable.sc displays a line through the **Start Time** and **Schedule** values.



Run a Diagnostic Scan

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

If you experience issues with an active scan, Tenable Support may ask you to run a diagnostic scan to assist with troubleshooting. After Tenable.sc runs the diagnostic scan, download the diagnostic file and send it to Tenable Support.

Before you begin:

- Add an active scan, as described in [Add an Active Scan](#).
- Confirm the scanner associated with the active scan is running a supported version of Nessus. For minimum Nessus scanner version requirements, see the [Tenable.sc Release Notes](#) for your version.

To run a diagnostic scan:

1. Click **Scans > Active Scans**.
2. In the row for the scan where you want to run a diagnostic scan, click the  menu.

The actions menu appears.

3. Click **Run Diagnostic Scan**.

Note: You must resolve repository errors before running a diagnostic scan.

4. In the **Diagnostic Target** box, type a target as a single IPv4 address, IPv6 address, or host-name. The target must also be specified in the active scan's **Targets**.
5. In the **Diagnostic Password** box, type a password to secure the diagnostic file.
6. Click **Submit**.

The diagnostic scan runs and finishes.

7. Click **Scans > Scan Results**.
8. Locate the diagnostic scan and confirm that the scan finished without errors.



9. In the row for the diagnostic scan result, click the  menu.

The actions menu appears.

10. Click **Download Diagnostic Info**.

The diagnostic scan file downloads.



Active Scan Settings

For more information, see [Add an Active Scan](#).

- [General Options](#)
- [Settings Options](#)
- [Targets Options](#)
- [Credentials Options](#)
- [Post Scan Options](#)

General Options

Parameter	Description
General	
Name	The scan name that is associated with the scan's results and may be any name or phrase (e.g., <i>SystemA</i> , <i>DMZ Scan</i> , <i>Daily Scan of the Web Farm</i> , etc.).
Description	Descriptive information related to the scan.
Policy	The policy on which you want to base the scan. You can scroll through the list, or search by entering text in the search box at the top of the list of available policies.
Schedule	
Schedule	The frequency you want to run the scan. • Now specifies that you want Tenable.sc to launch the scan immediately without saving the configuration for later. Note: Scans configured to run Now do not appear on the Active Scans page. • Once specifies that you want Tenable.sc to launch the scan at the specified time without saving the configuration for later.



Parameter	Description
	Note: Scans configured to run Once do not appear on the Active Scans page. • Daily, Weekly, or Monthly specifies that you want Tenable.sc to launch the scan at a scheduled interval. Note: If you schedule your scan to repeat monthly, Tenable recommends setting a start date no later than the 28th day. If you select a start date that does not exist in some months (e.g., the 29th), Tenable.sc cannot run the scan on those days. • On Demand specifies that you want to manually launch the scan at any time. • Dependent specifies that you want Tenable.sc to launch the scan every time Tenable.sc finishes a scheduled run of the dependent scan you select.

Settings Options

Parameter	Description
Basic	
Scan Zone	Note: If your organization's Distribution Method setting is Locked Zone, you cannot modify this setting. If your organization's Distribution Method setting is Automatic Distribution Only, this option is hidden because Tenable.sc automatically chooses one or more scan zones. Specifies the scan zone you want to use to run the scan. Depending on your organization's Distribution Method setting, you can select: • An available zone – use a single scan zone to run the scan. Note: If you select a single scan zone, Tenable.sc ignores the ranges in the scan zone and scans all of the targets you specify in the scan configuration. – or –



Parameter	Description
	• Automatic Distribution — allow Tenable.sc to choose the best scan zone to run the scan. For more information, see Organizations and Scan Zones.
Import Repository	Specifies the repository where the scan results are imported. Select a IPv4 or IPv6 repository to receive IPv4 or IPv6 results appropriate to the scan.
Scan Timeout Action	The action you want Tenable.sc to perform in the event a scan is incomplete: • Import Completed Results With Rollover — (Default option) The system imports the results from the scan into the database and creates a rollover scan that you can launch manually to complete the scan. • Import Completed Results — The system imports the results of the current scan and discards the information for the unscanned hosts. • Discard Results — The system does not import any of the results obtained by the scan to the database.
Rollover Schedule	If you set the Scan Timeout Action to Import results with Rollover , this option specifies how to handle the rollover scan. You can create the rollover scan as a template to launch manually, or to launch the next day at the same start time as the just-completed scan.
Advanced	
Scan Virtual Hosts	Specifies whether the system treats a new DNS entry for an IP address as a virtual host as opposed to a DNS name update. When a new DNS name is found for an IP address: • If you select this option, vulnerability data for the two DNS names appears as two entries with the same IP address in the IP Summary analysis tool.



Parameter	Description
	If you do not select this option, vulnerability data for the two DNS names merge into a single IP address entry in the IP Summary analysis tool.
Track hosts which have been issued new IP address	This option uses the DNS name, NetBIOS name, Agent ID, and MAC address (if known), in that order, to track a host when its IP address changes. Once a match has been made, Tenable.sc does not search further for matches. For example, if Tenable.sc does not match a DNS name, but it does match a NetBIOS name, the system does not check the MAC address. Networks using DHCP require that you set this option to properly track hosts.
Immediately remove vulnerabilities from scanned hosts that do not reply	If a previously responsive host does not reply to a scan, Tenable.sc removes the host's vulnerabilities from the cumulative database. If the host has vulnerabilities in the mitigated database, they remain in the mitigated database. - If you enable this option, the system removes the vulnerabilities immediately after the scan completes. - If you disable this option, the system removes the vulnerabilities according to the interval set in the Number of days to wait before removing dead hosts option.
Number of days to wait before removing dead hosts	If you disable Immediately remove vulnerabilities from scanned hosts that do not reply, this value specifies how many days the system waits to remove vulnerabilities.
Max scan duration (hours)	Specifies the maximum number of hours you want a scan to run. If a scan reaches this threshold, Tenable.sc automatically creates a rollover scan that you can launch manually to complete the scan. Tenable.sc creates a rollover scan regardless of your Scan Timeout Action setting.



Targets Options

The **Targets** section identifies the devices Tenable.sc scans.

Option	Description
Target Type	Specifies the target type for the scan: • Assets — Scan one or more assets. For more information, see Assets. • IP / DNS Name — Scan one or more IP addresses or DNS names. • Mixed—Scan a combination of asset lists, IP addresses, and DNS names.
Assets	(Available if Target Type is Assets or Mixed) The list of assets to scan. Click to select or deselect the assets you want to scan.
IPs / DNS Names	(Available if Target Type is IP / DNS Name or Mixed) The IP addresses or DNS names you want to scan. Specify IP addresses and DNS names using the following valid formats: • A single IPv4 address (for example, 192.0.2.202) • A single IPv6 address (for example, 2001:d-b8:d54e:cca6:4109:ac02:2fbe:134e) • An IP address range in dot-decimal or CIDR notation (for example, 192.0.2.0-192.0.2.255 or 192.0.2.0/24) • A resolvable hostname (for example, www.yourdomain.com) Note: You cannot scan both IPv4 and IPv6 addresses in the same scan, because you can only select one Import Repository.

Credentials Options

The **Credentials** section allows users to select pre-configured credential sets for authenticated scanning. For more information, see [Credentials](#).

Tenable.sc active scans support the following credential types:



- [Windows Credentials](#)
- [SSH Credentials](#)
- [SNMP Credentials](#)
- [Database Credentials](#)
- [API Gateway Credentials](#)

Post Scan Options

These options determine what actions occur immediately before and after the active scan completes.

Option	Description
Notifications	
E-mail me on Launch	This option specifies whether the system emails you a notification when the scan launches. This option only appears if you set an email address for your user account.
E-mail me on Completion	This option specifies whether the system emails you a notification when the scan completes. This option only appears if you set an email address for your user account.
Reports to Run on Scan Completion	
Add Report	This option provides a list of reports available to the user to run when the scan completes. The initial choices to select a report are to click the group and owner of the report to present a list of valid report options. Then click the report from the list that can be searched using the text search box. When hovering over a report name, you can select the information icon to display the name and description of the report. The report generated is based on the current scan's results or the results in the Cumulative database. Selecting the check mark causes that report to launch once the scan completes. Selecting the X removes the changes. Once added, you can modify or



Option	Description
	delete the report information.



Launch a Remediation Scan

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

You can run a remediation scan to run a followup active scan against existing active scan results. A remediation scan evaluates a specific plugin against a specific target or targets where the related vulnerability was present in your earlier active scan.

Remediation scans allow you to validate whether your vulnerability remediation actions on the targets have been successful. If a remediation scan cannot identify a vulnerability on targets where it was previously identified, the system changes the status of the vulnerability to mitigated. For more information, see [Cumulative vs. Mitigated Vulnerabilities](#).

Note the following:

- You can perform remediation scans only for active scan results.
- You cannot perform remediation scans for agent repository scan results.
- If the selected plugin requires dependent plugins, the system automatically includes those plugins in the remediation scan.
- Remediation scans only evaluate plugins against the port you specify. Keep this in mind when launching a remediation scan for a plugin that typically targets multiple ports.
- Remediation scans work best for un-credentialed network scan results. Use caution when running a remediation scan for a plugin that requires scan credentials. If you neglect to add scan credentials when required for a specific plugin, or if you mis-enter the credentials, the system may identify the related vulnerabilities as mitigated, not because they are mitigated, but because the system could not complete the credentialed scan.

To launch a remediation scan:

1. Log in to Tenable.sc via the user interface.
2. Click **Analysis > Vulnerabilities**.

The **Vulnerability Analysis** page appears.



3. Click the analysis tools drop-down box and select **Vulnerability Detail List**, **Vulnerability List**, or **Vulnerability Summary**.

The page refreshes to show the analysis tool view you selected.

4. In the row for the vulnerability you want to launch a remediation scan, click the  menu.

The actions menu appears.

5. Click **Launch Remediation Scan**.

The **Launch Remediation Scan** page appears.

A remediation scan inherits certain settings from the vulnerability or vulnerability instance you selected. The **Launch Remediation Scan** page:

- Automatically populates the relevant plugin information.
- Provides an editable scan name in the format "Remediation Scan of Plugin # *number*".
- Populates the target IP address based on the asset where the previous scan identified the vulnerability.

6. Configure the settings for the scan, as described in [Active Scan Settings](#).

Note: You do not need to associate the remediation scan with a scan policy.

Note: You cannot schedule a remediation scan. The scan launches as soon as you submit it.

7. Click **Submit**.

Tenable.sc launches the remediation scan.



Active Scan Objects

Complete Tenable.sc 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 (e.g., laptops, servers, tablets, phones, etc.) within a Tenable.sc organization. Assets can be shared with one or more users based on local security policy requirements. You can add an asset to group devices that share common attributes. Then, you can use the asset during scan configuration to target the devices in the asset. For more information, see Assets.
credentials	Credentials are reusable objects that facilitate a login to a scan target. Various types of credentials with different authentication methods can be configured for use within scan policies. Credentials may be shared between users for scanning purposes. Tenable.sc supports an unlimited number of SSH, Windows, and database credentials, and four SNMP credential sets per scan configuration. For more information, see Credentials.
audit files	During a configuration audit, auditors verify that servers and devices are configured according to an established standard and maintained with an appropriate procedure. Tenable.sc can perform configuration audits on key assets through the use of Nessus' local checks that can log directly onto a Unix or Windows server without an agent. Tenable.sc supports a variety of audit standards. Some of these come from best practice centers like the PCI Security Standards Council and the Center for Internet Security (CIS). Some of these are based on Tenable's interpretation of audit requirements to comply with specific industry standards such as PCI DSS or legislation such as Sarbanes-Oxley.



	In addition to base audits, it is easy to create customized audits for the particular requirements of any organization. These customized audits can be loaded into the Tenable.sc and made available to anyone performing configuration audits within an organization. NIST SCAP files can be uploaded and used in the same manner as an audit file. Navigate to NIST's SCAP website (http://scap.nist.gov) and under the SCAP Content section, download the desired SCAP security checklist zip file. The file may then be uploaded to Tenable.sc and selected for use in Nessus scan jobs. Once the audit scan policies are configured in Tenable.sc, they can be repeatedly used. Tenable.sc can also perform audits intended for specific assets. Through the use of audit policies and asset lists, a Tenable.sc user can quickly determine the compliance posture for any specified asset. For more information, see Audit Files.
scan zones	Scan zones represent areas of your network that you want to target in an active scan, associating an IP address or range of IP addresses with one or more scanners in your deployment. Scan zones define the IP address ranges associated with the scanner along with organizational access. For more information, see Scan Zones.
scan policies	Scan policies contain options related to performing an active scan. For example: • Options that control technical aspects of the scan such as timeouts, number of hosts, type of port scanner, and more. • Options that provide plugin family-based or individual plugin-based scan specifications. • Options that control compliance policy checks (Windows, Linux, Database, etc.), report verbosity, service detection scan settings, audit files, patch management systems, and more. For more information, see Scan Policies.



Assets

Tenable.sc assets are lists of devices (e.g., laptops, servers, tablets, phones, etc.) within a Tenable.sc organization. Assets can be shared with one or more users based on local security policy requirements.

You can add an asset to group devices that share common attributes. Then, you can use the asset during scan configuration to target the devices in the asset. Examples of common attributes include:

- IP address ranges
- hardware types
- vulnerabilities
- outdated software versions
- operating systems

Tenable.sc supports template-based and custom assets. For more information, see [Add a Template-Based Asset](#) and [Add a Custom Asset](#). To view details for any of your assets, see [View Asset Details](#).

Template-Based Assets

Tenable provides asset templates that you can customize for your environment. Tenable-provided asset templates are updated via the Tenable.sc feed and visible depending on other configurations.

Custom Assets

Tenable.sc supports the following custom assets types: [Static Assets](#), [DNS Name List Assets](#), [LDAP Query Assets](#), [Combination Assets](#), [Dynamic Assets](#), [Watchlist Assets](#), and [Import Assets](#).

Static Assets

Static assets are lists of IP addresses. You can use static assets immediately after configuration.

For example, if your organization assigns laptops within a defined IP address range, you can create a custom static asset for laptops using that IP address range.



Option	Description
Name	A name for the asset.
Description	A description for the asset.
Tag	A tag for the asset. For more information, see Tags .
IP Addresses	IP addresses to include within the asset (20,000 character limit). • Type a comma-delimited list of IP addresses, CIDR addresses, or ranges. • Upload a <code>.txt</code> file containing a comma-delimited list of IP addressees, CIDR addresses, or ranges.

DNS Name List Assets

Option	Description
Name	A name for the asset.
Description	A description for the asset.
DNS Names	The DNS hostnames for the asset to be based upon.

LDAP Query Assets

The LDAP query asset type appears if an LDAP server is configured within your organization.

Option	Description
Name	A name for the asset.
Description	A description for the asset.
LDAP Server	The LDAP server where you want to perform the query. Note: If the LDAP server is configured to use a different DNS server than Tenable.sc, Tenable.sc cannot resolve hostnames retrieved from the LDAP server.



Option	Description
	Note: Tenable.sc cannot retrieve more than one page of LDAP results. If Tenable.sc asset or user authentication queries are not retrieving all expected results, consider modifying your LDAP pagination control settings to increase the results per page.
Search Base	The LDAP search base used as the starting point to search for specific LDAP data.
Search String	This string may be modified to create a search based on a location or filter other than the default search base or attribute.
Generate Preview	The preview query is displayed in the Results Preview section after clicking Generate Preview . The preview lists the LDAP data that matches the defined search string.

Combination Assets

Combination assets allow you to create an asset based on existing assets and the AND, OR, and NOT operators.

Combination assets can include agent IDs if the asset contains exclusively dynamic assets. You may experience unexpected asset behavior if your combination asset contains other asset types and interacts with agent repository data.

Option	Description
Name	A name for the asset.
Description	A description for the asset.
Combination	This option accepts multiple existing assets utilizing the operators AND, OR, and NOT. Using these operators and multiple existing assets, new unique assets may be created. If the source assets change, the Combination asset updates to match the new conditions. When this option is initially selected, the options of NOT and a list of exist-



Option	Description
	ing assets are displayed. Selecting one of those options followed by a space will display the next valid option for building the asset and continue until the selections are complete. If the border for the combination option is red it is an indication that there is a problem in the logic of the query.

Dynamic Assets

Dynamic assets are flexible groups of condition statements that Tenable.sc uses to retrieve a list of devices meeting the conditions. Tenable.sc refreshes dynamic asset lists using the results from Tenable.sc scans. You cannot use dynamic assets until after Tenable.sc performs an initial discovery scan and retrieves a list of devices.

Dynamic assets can include agent IDs.

Add Dynamic Asset

← Back

General

Name*

Description

Tag

Asset Definition

All of the following are true:

Plugin ID

is equal to

✓ x

TCP Port

is equal to

80

Operating System

is equal to

Linux

Submit

Cancel

For example, in the asset above, Tenable.sc retrieves a list of Linux systems listening on TCP Port 80. For more information about constructing dynamic asset conditions, see [Dynamic Assets](#).



Option	Description
Name	A name for the asset.
Description	A description for the asset.
Asset Definition	Defines the rules for creating a dynamic asset list. Hovering over an existing rule will give the ability to add, edit, or delete a group or a rule to the definition.

Dynamic Asset 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 (e.g., 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 (e.g., ABCDEF contains ABC).
Posix regex	Any valid Posix regex pattern contained within "/" and "/" (e.g., /.*ABC.*/).
Perl compatible regex	Any valid Perl compatible regex pattern.
IP Address	
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 (e.g., 1.2.3.124 contains 124).
Posix regex	Any valid Posix regex pattern contained within "/" and "/" (e.g., /.*ABC.*/).
Perl compatible regex	Any valid Perl compatible regex pattern.
Port, TCP Port, UDP Port	
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	



Valid Operators	Effect
is equal to	Value must be equal to value specified. Scroll arrows are provided to allow for entry selection or the value can be manually entered. Max 365.
not equal to	Value must be not equal to value specified. Scroll arrows are provided to allow for entry selection or the value can be manually entered. Max 365.
is less than	Value is less than value specified. Scroll arrows are provided to allow for entry selection or the value can be manually entered. Max 365.
is greater than	Value is greater than the value specified. Scroll arrows are provided to allow for entry selection or the value can be manually entered. Max 365.
where Plugin ID is	Any valid Plugin ID number. Multiple Plugin IDs may be entered using a range and/or comma separated Plugin IDs (e.g., 3, 10189, 34598, 50000-55000, 800001-800055).
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).
where Plugin ID is	Any valid Plugin ID number. Multiple Plugin IDs may be entered using a range and/or comma separated Plugin IDs (e.g., 3, 10189, 34598, 50000-55000, 800001-800055).
Exploit Available	
Is	Click True or False in the drop-down box.
Exploit Frameworks	



Valid Operators	Effect
is equal to	Value must be equal to value specified.
Is not equal to	Value must not be equal to value specified.
contains the pattern	Value must contain the pattern entered.
XRef	
Value must be in the XRef option.	

Watchlist Assets

A watchlist is an asset that is used to maintain lists of IPs not in the user's managed range of IP addresses. IPs from a watchlist can be filtered on regardless of your IP address range configuration. This proves to be beneficial when analyzing event activity originating outside of the user's managed range. For example, if a block of IP addresses is a known source of malicious activity, it could be added to a Malicious IPs watchlist and added to a custom query.

Note: Watchlists only uses event data to create the asset list.

Option	Description
Name	A name for the asset.
Description	A description for the asset.
IP Addresses	IP addresses to include within the asset list (20,000 character limit). One address, CIDR address, or range can be entered per line. Click Choose File to import a list of IP addresses from a saved file.

Import Assets

Option	Description
Name	The asset name.
Asset	Click Choose File to choose the asset that was previously exported for import



Option	Description
	into Tenable.sc.



Add a Template-Based Asset

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

For information, see [Assets](#).

To add an asset from a Tenable-provided template:

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **Assets**.

The **Assets** page appears.

3. Click **Assets > Assets**.

The **Assets** page appears.

4. Click **Add**.

The **Add Assets** page appears.

The **Asset Templates** page appears.

5. (Optional) If you want to search for a specific asset template, type a search phrase in the **Search Templates** box.

6. In the **TemplatesCommon** section, click a template type.

The **Add Asset Template** page for the template type appears.

7. 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 NNM (PVS), LCE, and NS icons indicate you must have NNM, LCE, or Nessus data. The key icon () indicates you must have credentials for the device. The notepad icon () indicates you must have compliance data.

8. (Optional) If you want to search for a specific asset template, type a search phrase in the **Search Templates** box or select a category from the **All** drop-down box.



9. Click the row for the template you want to use.

The detail page for the template type appears.

10. Click **Add**.

The **Assets** page appears.

11. Click the row for the asset you just added.

The **Edit** page appears.

12. View the details for the asset.

13. (Optional) If necessary, edit the asset to customize it for your environment. For more information about asset options, see [Assets](#).

14. Click **Submit**.

Tenable.sc saves your configuration.



Add a Custom Asset

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

For information, see [Assets](#).

To add a custom asset:

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **Assets**.

The **Assets** page appears.

3. Click **Assets > Assets**.

The **Assets** page appears.

4. Click **Add**.

The **Add Assets** page appears.

The **Asset Templates** page appears.

5. In the **CustomOther** section, click an asset type.

The **Add Assets** page for the asset type appears.

6. Configure the required options for the asset type, as described in [Assets](#).
7. Click **Submit**.

Tenable.sc saves your configuration.



View Asset Details

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

You can view details for any asset. For more information, see [Assets](#).

To view asset details:

1. Log in to Tenable.sc via the user interface.
2. In the top navigation bar, click **Assets**.

The **Assets** page appears.

3. Click **Assets > Assets**.

The **Assets** page appears.

4. In the row for the asset you want to view, click the  menu.

The actions menu appears.

5. Click **View**.

The **View Asset** page appears.

Section	Action
General	View general information for the asset. • Name – The asset name. • Description – The asset description. • Tag – The tag applied to the asset. For more information, see Tags. • IP Addresses (static assets only) – The IP addresses specified in the asset. For more information, see Assets. • Created – The date the asset was created. • Last Modified – The date the asset was last modified.



Section	Action
	• Owner – The username for the user who created the asset. • Group – The group in which the asset belongs. • ID – The asset ID.
Tenable.io Syn- chronization Data	View synchronization summary data: • Status – The status of the asset in Lumin synchronization: • Finished – The most recent synchronization that included this asset succeeded. • Not Synced – The asset is not configured for Lumin synchronization. • Error – An error occurred. For more information, see View Lumin Data Synchronization Logs. • First Synchronization – The date and time of the first synchronization of this asset. • Last Success – The date and time of the most recent synchronization of this asset. • Last Failure – The date and time of the most recent failed synchronization of this asset. • Details – If the Status is Error, details about the error. For more information about Lumin synchronization, see Lumin Synchronization.



Credentials

Credentials are reusable objects that facilitate scan target login.

Administrators can add credentials available to all organizations. Organizational users can add credentials available to other users in the same organization. For information about user access in Tenable.sc, see [User Access](#).

Users can share credentials with other users, allowing them to scan remote hosts without knowing the credentials of the host. For information about Tenable.sc credential data encryption, see [Encryption Strength](#).

Tenable.sc supports the following credential types:

- [API Gateway Credentials](#)
- [Database Credentials](#)
- [SNMP Credentials](#)
- [SSH Credentials](#)
- [Windows Credentials](#)

If a scan contains multiple instances of one type of credential, Tenable.sc tries the credentials on each scan target in the order you added the credentials to the scan.

Note: Tenable.sc uses the first credential that allows successful login to perform credentialed checks on the target. After a credential allows a successful login, Tenable.sc does not try any of the other credentials in the list, even if a different credential has greater privileges.

To add credentials, see [Add Credentials](#).



Add Credentials

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

For more information about credentials, see [Credentials](#).

Note: You can add up to 1000 SSH credentials in a single scan. For best performance, Tenable recommends adding no more than 10 SSH credentials per scan.

To add credentials:

1. Log in to Tenable.sc.
2. Click **Scanning > Credentials** (administrator users) or **Scans > Credentials** (organizational users).

The **Credentials** page appears.

3. Click **Add**.

The **Add Credential** page appears.

The **Credential Templates** page appears.

4. In the **API Gateway**, **Database**, **SNMP**, **SSH**, or **Windows** sections, click the tile for the specific method you want to configure.

The **Add Credentials** configuration page appears.

5. In the **Name** box, type a name for the credentials.
6. In the **Description** box, type a description for the credentials.
7. (Optional) Type or select a **Tag**. For more information, see [Tags](#).
8. Configure the options, as described in:

- [API Gateway Credentials](#)
- [Database Credentials](#)
- [SNMP Credentials](#)



- [SSH Credentials](#)
- [Windows Credentials](#)

9. Click **Submit**.

Tenable.sc saves your configuration.



API Gateway Credentials

Configure the following options for all API gateway credentials.

Option	Description
Name (Required)	A name for the credential.
Description	A description for the credential.
Tag	A tag for the credential. For more information, see Tags .

IBM DataPower Options

The following table describes the additional options to configure for **IBM DataPower** credentials.

Option	Description
Client Certificate	The file that contains the PEM certificate used to communicate with the IBM DataPower host.
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.
Custom Header Key	If your IBM DataPower configuration uses custom HTTP headers, the custom HTTP header key.
Custom Header Value	If your IBM DataPower configuration uses custom HTTP headers, the custom HTTP header value.
Enable for Hashicorp Vault	When enabled, allows Tenable.sc to use the IBM DataPower credential with a Hashicorp Vault credential. Tip: If you want to run a test that does not use IBM DataPower credentials



Option	Description
	without having to delete the credential, you can temporarily disable this option to prevent Tenable.sc from using IBM DataPower credentials.



Database Credentials

The following are available **Database** credentials:

- [IBM DB2](#)
- [Informix/DRDA](#)
- [MySQL](#)
- [Oracle Database](#)
- [PostgreSQL](#)
- [SQL Server](#)
- [MongoDB](#)
- [Apache Cassandra](#)

Note: Aspects of credential options are based on Nessus plugin options. Therefore, specific credential options may differ from the descriptions documented here.

Configure the following options for all database credentials:

Options	Description
Name (Required)	A name for the credential.
Description	A description for the credential.
Tag	A tag for the credential. For more information, see Tags .

IBM DB2

The following table describes the additional options to configure for **IBM DB2** credentials.

Options	Description
Source	The method for providing the required credential details: Entry or Import .



Options	Description
	• Entry – Specifies you want to use a single SID value or SERVICE_NAME value for the credential. You must also configure the remaining options on the Add Credential page, as described in Add Credentials. • Import – Specifies you want to use multiple SID values for the credential, uploaded as a .csv file. For more information about the required .csv file format, see Database Credentials Authentication.
Authentication Method	The authentication method for providing the required credentials. • CyberArk • Password • Lieberman • Hashicorp Vault For descriptions of the options for your selected authentication type, see Database Credentials Authentication.
Port	The TCP port that the IBM DB2 database instance listens on for communications from Tenable.sc. The default is port 50000.
Database Name	The name for your database (not the name of your instance).

Informix/DRDA

The following table describes the additional options to configure for **Informix/DRDA** credentials.

Options	Description
Username	The username for a user on the database.
Password	The password associated with the username you provided.



Options	Description
Port	The TCP port that the Informix/DRDA database instance listens on for communications from Tenable.sc. The default is port 1526.

MySQL

The following table describes the additional options to configure for **MySQL** credentials.

Options	Description
Source	The method for providing the required credential details: Entry or Import. • Entry — Specifies you want to use a single SID value or SERVICE_NAME value for the credential. You must also configure the remaining options on the Add Credential page, as described in Add Credentials. • Import — Specifies you want to use multiple SID values for the credential, uploaded as a .csv file. For more information about the required .csv file format, see Database Credentials Authentication.
Authentication Method	The authentication method for providing the required credentials. • CyberArk • Password • Lieberman • Hashicorp Vault For descriptions of the options for your selected authentication type, see Database Credentials Authentication.
Username	The username for a user on the database.



Options	Description
Password	The password associated with the username you provided.
Port	The TCP port that the MySQL database instance listens on for communications from Tenable.sc. The default is port 3306.
SID	The name for your database instance.

Oracle Database

The following table describes the additional options to configure for **Oracle Database** credentials.

Options	Description
Source	The method for providing the required credential details: Entry or Import. • Entry — Specifies you want to use a single SID value or SERVICE_NAME value for the credential. You must also configure the remaining options on the Add Credential page, as described in Add Credentials. • Import — Specifies you want to use multiple SID values for the credential, uploaded as a .csv file. For more information about the required .csv file format, see Database Credentials Authentication.
Authentication Method	The authentication method for providing the required credentials. • CyberArk • Password • Lieberman • Hashicorp Vault For descriptions of the options for your selected authentication type, see Database Credentials Authentication.



Options	Description
Port	The TCP port that the Oracle database instance listens on for communications from Tenable.sc. The default is port 1521.
Authentication	The type of account you want Tenable.sc to use to access the database instance: • Normal • System Operator • System Database Administrator
Service Type	The Oracle parameter you want to use to specify the database instance: SID or Service Name .
Service	The SID value or SERVICE_NAME value for your database instance. The Service value you enter must match your parameter selection for the Service Type option.

PostgreSQL

The following table describes the additional options to configure for **PostgreSQL** credentials.

Options	Description
Authentication Method	The authentication method for providing the required credentials. • CyberArk • Password • Lieberman • Hashicorp Vault For descriptions of the options for your selected authentication type, see Database Credentials Authentication.



Options	Description
Port	The TCP port that the PostgreSQL database instance listens on for communications from Tenable.sc. The default is port 5432.
Database Name	The name for your database instance.

SQL Server

The following table describes the additional options to configure for **SQL Server** credentials.

Options	Description
Source	The method for providing the required credential details: Entry or Import. • Entry – Specifies you want to use a single SID value or SERVICE_NAME value for the credential. You must also configure the remaining options on the Add Credential page, as described in Add Credentials. • Import – Specifies you want to use multiple SID values for the credential, uploaded as a .csv file. For more information about the required .csv file format, see Database Credentials Authentication.
Authentication Method	The authentication method for providing the required credentials. • CyberArk • Password • Lieberman • Hashicorp Vault For descriptions of the options for your selected authentication type, see Database Credentials Authentication.



Options	Description
Username	The username for a user on the database.
Password	The password associated with the username you provided.
Port	The TCP port that the SQL Server database instance listens on for communications from Tenable.sc. The default is port 1433.
Authentication	The type of account you want Tenable.sc to use to access the database instance: SQL or Windows .
Instance Name	The name for your database instance.

MongoDB

Option	Description
Username	The username for the database.
Password	The password for the supplied username.
Database	The name of the database to audit.
Port	(Required) The TCP port that the MongoDB database instance listens on for communications from Tenable.sc.



Database Credentials Authentication Method Settings

Depending on the authentication type you select for your database credentials, you must configure the following options. For more information about database credential settings, see [Database Credentials](#).

- [Import](#)
- [CyberArk Options](#)
- [Password Options](#)
- [Lieberman Options](#)
- [Hashicorp Vault Options](#)

Import

Upload a .csv file with the credentials entered in the specified format. For descriptions of valid values to use for each item, see [Database Credentials](#).

You must configure either CyberArk or HashiCorp credentials for a database credential in the same scan so that Tenable.sc can retrieve the credentials.

Database Credential	CSV Format
IBM DB2	target, port, database_name, username, cred_manager, accountname_or_secretname
MySQL	target, port, database_name, username, cred_manager, accountname_or_secretname
Oracle	target, port, service_type, service_ID, username, auth_type, cred_manager, accountname_or_secretname
SQL Server	target, port, instance_name, username, auth_type, cred_manager, accountname_or_secretname

Note: Include the required data in the specified order, with commas between each value, without spaces. For example, for Oracle with CyberArk: 192.0.2.255,1521,SID,service_id,username,SYSDBA,CyberArk,Database-Oracle-SYS.



Note: The value for `cred_manager` must be either *CyberArk* or *HashiCorp*.

CyberArk Options

The following table describes the additional options to configure when using CyberArk as the **Authentication Method** for **IBM DB2**, **SQL Server**, **MySQL**, **Oracle Database**, or **PostgreSQL** database credentials.

Note: You must be running Nessus 7.0.0 or later to configure CyberArk credentials.

Option	Database Types	Description
Username	All	The username for the target system.
Port	All	The port the database is listening on.
Service Type	Oracle Database	The Oracle parameter you want to use to identify the database instance: SID or Service Name .
Service	Oracle Database	The SID value for your database instance or a SERVICE_NAME value. The Service value you enter must match your parameter selection for the Service Type option.
Database Name	IBM D2 Postgre SQL	The name for your database instance.
Central Credential Provider URL Host	All	The IP/DNS address of the CyberArk Central Credential Provider.
Central Credential Provider URL Port	All	The port the CyberArk Central Credential Provider is listening on.
Vault User-	All	The username for the vault, if the CyberArk Central Cre-



Option	Database Types	Description
name		dential Provider is configured for basic authentication.
Vault Password	All	The password for the vault, if the CyberArk Central Credential Provider is configured for basic authentication.
Safe	All	The safe on the CyberArk Central Credential Provider server that contains the credentials you want to retrieve.
CyberArk Client Certificate	All	The file that contains the PEM certificate used to communicate with the CyberArk host.
CyberArk Client Certificate Private Key	All	The file that contains the PEM private key for the client certificate.
CyberArk Client Certificate Private Key Passphrase	All	The passphrase for the private key, if required.
AppID	All	The AppID with CyberArk Central Credential Provider permissions to retrieve the target password.
Folder	All	The folder on the CyberArk Central Credential Provider server that contains the credentials you want to retrieve.
PolicyID	All	
Vault Use SSL	All	When enabled, Tenable.sc uses SSL through IIS for secure communications. You must configure SSL through IIS in CyberArk Central Credential Provider before enabling this option.
Vault Verify SSL	All	When enabled, Tenable.sc validates the SSL certificate. You must configure SSL through IIS in CyberArk Central Credential Provider before enabling this option.



Option	Database Types	Description
		For more information about using self-signed certificates, see the Nessus custom_CA.inc documentation.
CyberArk AIM Service URL	All	The URL for the CyberArk AIM web service. By default, Tenable.sc uses <code>/AIMWebservice/v1.1/AIM.asmx</code> .

Password Options

The following table describes the additional options to configure when using Password as the **Authentication Method** for database credentials.

Option	Database Types	Description
Username	All	The username for a user on the database.
Password	All	The password associated with the username you provided.
Port	All	The port the database is listening on.
Database Name	IBM D2 PostgreSQL	The name for your database instance.
Authentication	Oracle Database SQL Server	The type of account you want Tenable.sc to use to access the database instance.
Service Type	Oracle Database	The Oracle parameter you want to use to identify the database instance: SID or Service Name .
Service	Oracle Database	The SID value for your database instance or a SERVICE_NAME value. The Service value you enter must match your parameter selection for the Service Type option.



Option	Database Types	Description
Instance Name	SQL Server	The name for your database instance.

Lieberman Options

The following table describes the additional options to configure when using Lieberman as the **Authentication Method** for **IBM DB2**, **SQL Server**, **MySQL**, **Oracle Database**, or **PostgreSQL** database credentials.

Note: You must meet the version requirements specified in [Tenable Integrated Product Compatibility](#).

Option	Database Types	Description
Username	All	The username for a user on the database.
Port	All	The port the database is listening on.
Database Name	IBM DB2 PostgreSQL	The name for your database instance.
Authentication	Oracle Data-base SQL Server	The type of account you want Tenable.sc to use to access the database instance.
Service Type	Oracle Data-base	The Oracle parameter you want to use to identify the database instance: SID or Service Name .
Service	Oracle Data-base	The SID value for your database instance or a SERVICE_NAME value. The Service value you enter must match your parameter selection for the Service Type option.
Instance Name	SQL Server	The name for your database instance.



Option	Database Types	Description
Lieberman Host	All	The Lieberman IP address or DNS address.
Lieberman Port	All	The port Lieberman is listening on.
Lieberman User	All	The username for the Lieberman explicit user you want Tenable.sc to use for authentication to the Lieberman Rapid Enterprise Defense (RED) API.
Lieberman Password	All	The password for the Lieberman explicit user.
Use SSL	All	When enabled, Tenable.sc uses SSL through IIS for secure communications. You must configure SSL through IIS in Lieberman before enabling this option.
Verify SSL Certificate	All	When enabled, Tenable.sc validates the SSL certificate. You must configure SSL through IIS in Lieberman before enabling this option.
System Name	All	The name for the database credentials in Lieberman.

Hashicorp Vault Options

The following table describes the additional options to configure when using Hashicorp Vault as the **Authentication Method** for **IBM DB2**, **SQL Server**, **MySQL**, **Oracle Database**, or **PostgreSQL** database credentials.

Option	Credential	Description	Required
Port	Oracle Database IBM DB2 MySQL PostgreSQL	The port on which Tenable.sc communicates with the database.	yes



	SQL Server		
SID	MySQL	The security identifier used to connect to the database.	yes
Database Name	IBM DB2 PostgreSQL	The name of the database.	no
Instance Name	SQL Server	The SQL server name.	yes
Hashicorp Host	All	The Hashicorp Vault IP address or DNS address. Note: If your Hashicorp Vault installation is in a subdirectory, you must include the subdirectory path. For example, type <i>IP address or host-name/subdirectory path</i>.	yes
Hashicorp Port	All	The port on which Hashicorp Vault listens.	yes
Service Type	Oracle Database	The unique SID or Service Name that identifies your database.	yes
Service	Oracle Database	The SID or Service Name value for your database instance. Note: The Service value must match the Service Type option parameter selection.	yes
Authentication Type	All	Specifies the authentication type for connecting to the instance: App Role or Certificates .	yes
Client Cert	All	If Authentication Type is Cer-	yes



		tificates , the client certificate file you want to use to authenticate the connection.	
Private Key	All	If Authentication Type is Certificates , the private key file associated with the client certificate you want to use to authenticate the connection.	yes
Role ID	All	The GUID provided by Hashicorp Vault when you configured your App Role.	yes
Role Secret ID	All	The GUID generated by Hashicorp Vault when you configured your App Role.	yes
Authentication URL	All	The URL Tenable.sc uses to access Hashicorp Vault.	yes
Namespace	All	The name of a specified team in a multi-team environment.	no
Hashicorp Vault Type	All	The type of Hashicorp Vault secrets engine: • KV1 – Key/Value Secrets Engine Version 1 • KV2 – Key/Value Secrets Engine Version 2 • AD – Active Directory	yes
KV Engine URL	All	The URL Tenable.sc uses to access the Hashicorp Vault secrets engine.	yes
Username Source	All	(Only displays if Hashicorp	yes



		Vault Type is KV1 or KV2) Specifies if the username is input manually or pulled from Hashicorp Vault.	
Username key	All	(Only displays if Hashicorp Vault Type is KV1 or KV2) The name in Hashicorp Vault that usernames are stored under.	no
Username	All	(Only displays if Username Source is Manual Entry) The name in Hashicorp Vault that usernames are stored under.	yes
Password key	All	(Only displays if Hashicorp Vault Type is KV1 or KV2) The key in Hashicorp Vault that passwords are stored under.	no
Secret Name	All	The key secret you want to retrieve values for.	yes
Use SSL	All	When enabled, Tenable.sc uses SSL for secure communications. You must configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL	All	When enabled, Tenable.sc validates the SSL certificate. You must configure SSL in Hashicorp Vault before enabling this option.	no



SNMP Credentials

Configure the following options for SNMP credentials. Tenable.sc supports SNMPv1 for authentication via a community string.

Options	Description
Name	(Required) A name for the credential.
Description	A description for the credential.
Tag	A tag for the credential. For more information, see Tags .
Community	The SNMP community string used for authentication.



SSH Credentials

Use SSH credentials for host-based checks on Unix systems and supported network devices. Tenable.sc uses these credentials to obtain local information from remote Unix systems for patch auditing or compliance checks. Tenable.sc uses Secure Shell (SSH) protocol version 2 based programs (e.g., OpenSSH, Solaris SSH, etc.) for host-based checks.

Tenable.sc encrypts the data using the AES-256-CBC algorithm to protect it from being viewed by sniffer programs.

Note: Non-privileged users with local access on Linux systems can determine basic security issues, such as patch levels or entries in the `/etc/passwd` file. For more comprehensive information, such as system configuration data or file permissions across the entire system, an account with root privileges is required.

Note: You can add up to 1000 SSH credentials in a single scan. For best performance, Tenable recommends adding no more than 10 SSH credentials per scan.

Configure the following options for SSH credentials, including options specific for your authentication method: [Arcon Options](#), [Certificate Options](#), [CyberArk Vault Options](#), [Hashicorp Vault Options](#), [Kerberos Options](#), [Password Options](#), [Public Key Options](#), [Thycotic Secret Server Options](#), [BeyondTrust Options](#), and [Lieberman Options](#).

General Option	Description
Name	(Required) A name for the credential.
Description	A description for the credential.
Tag	A tag for the credential. For more information, see Tags .

Arcon Options

The following table describes the additional options to configure when using **Arcon** as the authentication method for SSH credentials.

Option	Description
Arcon Host	(Required) The Arcon IP address or DNS address.



	Note: If your Arcon installation is in a subdirectory, you must include the subdirectory path. For example, type <i>IP address or hostname/subdirectory path</i> .
Arcon Port	(Required) The port on which Arcon listens. By default, Tenable.sc uses port 444.
API User	(Required) The API user provided by Arcon.
API Key	(Required) The API key provided by Arcon.
Authentication URL	(Required) The URL Tenable.sc uses to access Arcon.
Password Engine URL	(Required) The URL Tenable.sc uses to access the passwords in Arcon.
Username	(Required) The username to log in to the hosts you want to scan.
Checkout Duration	(Required) The length of time, in minutes, that you want to keep credentials checked out in Arcon. Configure the Checkout Duration to exceed the typical duration of your Tenable.sc scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. Tip: Configure the password change interval in Arcon so that password changes do not disrupt your Tenable.sc scans. If Arcon changes a password during a scan, the scan fails.
Use SSL	When enabled, Tenable.sc uses SSL through IIS for secure communications. You must configure SSL through IIS in Arcon before enabling this option.
Verify SSL Certificate	When enabled, Tenable.sc validates the SSL certificate. You must configure SSL through IIS in Arcon before enabling this option.

Certificate Options



The following table describes the additional options to configure when using **Certificate** as the authentication method for SSH credentials.

Option	Description
Username	(Required) The username for a user on the host system.
User Certificate	(Required) The RSA or DSA OpenSSH certificate file for the user.
Private Key	(Required) The RSA or DSA OpenSSH private key file for the user.
Passphrase	The passphrase for the private key, if required.
Privilege Escalation	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your Privilege Escalation selection determines the specific options you must configure. For more information, see Privilege Escalation .

CyberArk Vault Options

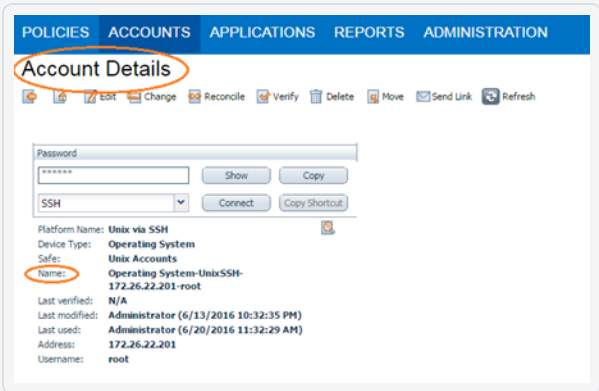
The following table describes the additional options to configure when using **CyberArk Vault** as the authentication method for SSH credentials.

Option	Description
Username	(Required) The username for the target system.
CyberArk elevate privileges with	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your CyberArk elevate privileges with selection determines the specific options you must configure. For more information, see Privilege Escalation .
Central Credential Provider URL Host	(Required) The CyberArk Central Credential Provider IP/DNS address.
Central Credential Provider URL Port	(Required) The port the CyberArk Central Credential Provider is listening on.



Option	Description
CyberArk Address	The domain for the CyberArk account. You must configure SSL through IIS in CyberArk Central Credential Provider before configuring this option.
Vault Username	The username for the vault, if the CyberArk Central Credential Provider is configured for basic authentication.
Vault Password	The password for the vault, if the CyberArk Central Credential Provider is configured for basic authentication.
Safe	The safe on the CyberArk Central Credential Provider server that contains the credentials you want to retrieve.
CyberArk Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host.
CyberArk Client Certificate Private Key	The file that contains the PEM private key for the client certificate.
CyberArk Client Certificate Private Key Passphrase	The passphrase for the private key, if required.
AppID	(Required) The AppID with CyberArk Central Credential Provider permissions to retrieve the target password.
Folder	The folder on the CyberArk Central Credential Provider server that contains the credentials you want to retrieve.
PolicyID	The PolicyID assigned to the credentials you want to retrieve.
Vault Use SSL	When enabled, Tenable.sc uses SSL through IIS for secure communications. You must configure SSL through IIS in CyberArk Central Credential Provider before enabling this option.
Vault Verify SSL	When enabled, Tenable.sc validates the SSL certificate. You must configure SSL through IIS in CyberArk Central Credential Provider before enabling this



Option	Description
	option.
CyberArk Escalation Account Details Name	The unique name of the credential you want to retrieve from CyberArk. 
CyberArk AIM Service URL	The URL for the CyberArk AIM web service. By default, Tenable.sc uses /AIMWebservice/v1.1/AIM.asmx.

Hashicorp Vault Options

The following table describes the additional options to configure when using **Hashicorp Vault** as the authentication method for SSH credentials.

Option	Default Value	Required
Hashicorp Host	The Hashicorp Vault IP address or DNS address. Note: If your Hashicorp Vault installation is in a sub-directory, you must include the subdirectory path. For example, type <i>IP address or hostname/subdirectory path</i>.	yes
Hashicorp Port	The port on which Hashicorp Vault listens.	yes
Authentication Type	Specifies the authentication type for connecting to the instance: App Role or Certificates. If you select Certificates, additional options for	yes



	Hashicorp Client Certificate (Required) and Hashicorp Client Certificate Private Key (Required) appear. Select the appropriate files for the client certificate and private key.	
Role ID	The GUID provided by Hashicorp Vault when you configured your App Role.	yes
Role Secret ID	The GUID generated by Hashicorp Vault when you configured your App Role.	yes
Authentication URL	The URL used to access Hashicorp Vault.	yes
Namespace	The name of a specified team in a multi-team environment.	no
Hashicorp Vault Type	The type of Hashicorp Vault secrets engine: • KV1 – Key/Value Secrets Engine Version 1 • KV2 – Key/Value Secrets Engine Version 2 • AD – Active Directory	yes
KV Engine URL	The URL Tenable.sc uses to access the Hashicorp Vault secrets engine.	yes
Username Source	(Only displays if Hashicorp Vault Type is KV1 or KV2) Specifies if the username is input manually or pulled from Hashicorp Vault.	yes
Username key	(Only displays if Hashicorp Vault Type is KV1 or KV2) The name in Hashicorp Vault that usernames are stored under.	yes
Password key	(Only displays if Hashicorp Vault Type is KV1 or KV2) The key in Hashicorp Vault that passwords are stored under.	yes



Secret Name	The key secret you want to retrieve values for.	yes
Use SSL	When enabled, Tenable.sc uses SSL for secure communications. You must configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL	When enabled, Tenable.sc validates the SSL certificate. You must configure SSL in Hashicorp Vault before enabling this option.	no

Kerberos Options

The following table describes the additional options to configure when using **Kerberos** as the authentication method for SSH credentials.

Option	Description
Username	(Required) The username for a user on the target system.
Password	(Required) The password associated with the username you provided.
KDC Host	(Required) The host supplying the session tickets.
KDC Port	(Required) The port you want to use for the KDC connection. By default, Tenable.sc uses port 88.
KDC Transport	(Required) The method you want to use to connect to the KDC server. Note: If you select UDP, you may need to edit the KDC Port. The KDC UDP protocol uses either port 88 or port 750.
Realm	(Required) The authentication domain, typically the domain name of the target (e.g., <i>example.com</i>).
Privilege Escalation	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your Privilege Escalation selection determines the specific options you must configure. For more information, see Privilege Escalation .

Password Options



The most effective credentialed scans are those with root privileges (enable privileges, for Cisco IOS). Since many sites do not permit a remote login as root for security reasons, a Nessus user account can invoke a variety of privilege escalation options including: `su`, `sudo`, `su+sudo`, `DirectAuthorize` (`dzdo`), `PowerBroker` (`pbrun`), `k5login`, and `Cisco Enable`.

The following table describes the additional options to configure when using **Password** as the authentication method for SSH credentials.

Option	Description
Username	(Required) The username for a user on the target system.
Password	(Required) The password associated with the username you provided.
Privilege Escalation	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your Privilege Escalation selection determines the specific options you must configure. For more information, see Privilege Escalation .

Public Key Options

The following table describes the additional options to configure when using **Public Key** as the authentication method for SSH credentials.

Option	Description
Username	(Required) The username for a user on the host system.
Private Key	(Required) The RSA or DSA OpenSSH key file for the user.
Passphrase	The passphrase for the private key, if required.
Privilege Escalation	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your Privilege Escalation selection determines the specific options you must configure. For more information, see Privilege Escalation .

Thycotic Secret Server Options



The following table describes the additional options to configure when using **Thycotic Secret Server** as the authentication method for SSH credentials.

Option	Description
Username	(Required) The username for a user on the target system.
Thycotic Secret Name	The Secret Name value on the Thycotic server.
Thycotic Secret Server URL	(Required) The value you want Tenable.sc to use when setting the transfer method, target, and target directory for the scanner. Find the value on the Thycotic server, in Admin > Configuration > Application Settings > Secret Server URL. For example, if you type <i>https://pw.mydomain.com/SecretServer</i>, Tenable.sc determines it is an SSL connection, that <i>pw.mydomain.com</i> is the target address, and that <i>/SecretServer</i> is the root directory.
Thycotic Login Name	(Required) The username for a user on the Thycotic server.
Thycotic Password	(Required) The password associated with the Thycotic Login Name you provided.
Thycotic Organization	In cloud instances of Thycotic, the value that identifies the organization you want Tenable.sc to target.
Thycotic Domain	The domain, if set for the Thycotic server.
Verify SSL Certificate	If enabled, Tenable.sc verifies the SSL Certificate on the Thycotic server. For more information about using self-signed certificates, see the Nessus custom_CA.inc documentation.
Use Private Key	If enabled, Tenable.sc uses key-based authentication for SSH connections instead of password authentication.

BeyondTrust Options



The following table describes the additional options to configure when using **BeyondTrust** as the authentication method for SSH credentials.

Option	Description
Username	The username to log in to the hosts you want to scan.
BeyondTrust Host	The BeyondTrust IP address or DNS address.
BeyondTrust Port	The port BeyondTrust is listening on.
BeyondTrust API User	The API user provided by BeyondTrust.
BeyondTrust API Key	The API key provided by BeyondTrust.
Checkout Duration	The length of time, in minutes, that you want to keep credentials checked out in BeyondTrust. Configure the Checkout duration to exceed the typical duration of your Tenable.sc scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. Tip: Configure the password change interval in BeyondTrust so that password changes do not disrupt your Tenable.sc scans. If BeyondTrust changes a password during a scan, the scan fails.
Use SSL	If enabled, Tenable.sc uses SSL through IIS for secure communications. You must configure SSL through IIS in BeyondTrust before enabling this option.
Verify SSL Certificate	If enabled, Tenable.sc validates the SSL certificate. You must configure SSL through IIS in BeyondTrust before enabling this option.
Use Private Key	If enabled, Tenable.sc uses key-based authentication for SSH connections instead of password authentication.
Use Privilege Escalations	If enabled, Tenable.sc uses BeyondTrust for privilege escalation.



Lieberman Options

The following table describes the additional options to configure when using **Lieberman** as the authentication method for SSH credentials.

Option	Description
Username	The username for a user on the database.
Lieberman Host	The Lieberman IP address or DNS address. Note: If your Lieberman installation is in a subdirectory, you must include the subdirectory path. For example, type <i>IP address or hostname/sub-directory path</i>.
Lieberman Port	The port Lieberman is listening on.
Lieberman User	The username for the Lieberman explicit user you want Tenable.sc to use for authentication to the Lieberman Rapid Enterprise Defense (RED) API.
Lieberman Password	The password for the Lieberman explicit user.
Use SSL	When enabled, Tenable.sc uses SSL through IIS for secure communications. You must configure SSL through IIS in Lieberman before enabling this option.
Verify SSL Certificate	When enabled, Tenable.sc validates the SSL certificate. You must configure SSL through IIS in Lieberman before enabling this option.
System Name	The name for the database credentials in Lieberman.



Privilege Escalation

Some SSH credential types support privilege escalation.

Note: BeyondTrust's PowerBroker (pbrun) and Centrify's DirectAuthorize (dzdo) are proprietary root task delegation methods for Unix and Linux systems.

Tip: Scans run using su+sudo allow the user to scan with a non-privileged account and then switch to a user with sudo privileges on the remote host. This is important for locations where remote privileged login is prohibited.

Note: Scans run using sudo vs. the root user do not always return the same results because of the different environmental variables applied to the sudo user and other subtle differences. For more information, see <https://www.sudo.ws/man/sudo.man.html>.

The following table describes the additional options to configure for privilege escalation.

Option	SSH Types	Description
Escalation Username	Kerberos	The username for the account with elevated privileges.
	Password	
	Public Key	
Escalation Password	Kerberos	The password for the account with elevated privileges.
	Password	
	Public Key	
Escalation Path	Kerberos	The directory path for the privilege escalation commands.
	Password	
	Public Key	
Escalation Su User	CyberArk	The username for the account with su privileges.
	Kerberos	
	Password	
	Public Key	



Option	SSH Types	Description
CyberArk Escalation Account Details Name	CyberArk	The name parameter for the CyberArk account with elevated privileges. Note: The system uses the password associated with the CyberArk account name you provide for all scanned hosts.
Escalation Account	CyberArk	The username for the account with elevated privileges.
Escalation sudo user	CyberArk	The username for the account with sudo privileges.
Location of dzdo (directory)	CyberArk	The directory path for the dzdo command.
Location of pbrun (directory)	CyberArk	The directory path for the pbrun command.
Location of su (directory)	CyberArk	The directory path for the su command.
Location of su and sudo (directory)	CyberArk	The directory path for the su and sudo commands.
Location of sudo (directory)	CyberArk	The directory path for the sudo command.
su login	CyberArk	The username for the account with su privileges.
sudo login	CyberArk	The username for the account with sudo privileges.



Windows Credentials

Nessus has vulnerability checks that can use a Microsoft Windows domain account to find local information from a remote Windows host. For example, using credentials enables Nessus to determine if important security patches have been applied.

Tip: Using a non-administrator account will greatly affect the quality of the scan results. Often it makes sense to create a special Nessus user with administrative privileges that is used solely for scheduled scanning.

Configure the following options for Windows credentials, including options specific for your authentication method: [Arcon Options](#), [CyberArk Vault Options](#), [Hashicorp Vault Options](#), [Kerberos Options](#), [LM Hash Options](#), [NTLM Hash Options](#), [Password Options](#), [Thycotic Secret Server Options](#), [BeyondTrust Options](#), and [Lieberman Options](#).

General Options	Description
Name	(Required) A name for the credential.
Description	A description for the credential.
Tag	A tag for the credential. For more information, see Tags .

Arcon Options

The following table describes the additional options to configure when using **Arcon** as the authentication method for Windows credentials.

Option	Description
Arcon Host	(Required) The Arcon IP address or DNS address. Note: If your Arcon installation is in a subdirectory, you must include the subdirectory path. For example, type <i>IP address or hostname/subdirectory path</i>.
Arcon Port	(Required) The port on which Arcon listens. By default, Tenable.sc uses port 444.



API User	(Required) The API user provided by Arcon.
API Key	(Required) The API key provided by Arcon.
Authentication URL	(Required) The URL Tenable.sc uses to access Arcon.
Password Engine URL	(Required) The URL Tenable.sc uses to access the passwords in Arcon.
Username	(Required) The username to log in to the hosts you want to scan.
Checkout Duration	(Required) The length of time, in minutes, that you want to keep credentials checked out in Arcon. Configure the Checkout Duration to exceed the typical duration of your Tenable.sc scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. Tip: Configure the password change interval in Arcon so that password changes do not disrupt your Tenable.sc scans. If Arcon changes a password during a scan, the scan fails.
Use SSL	When enabled, Tenable.sc uses SSL through IIS for secure communications. You must configure SSL through IIS in Arcon before enabling this option.
Verify SSL Certificate	When enabled, Tenable.sc validates the SSL certificate. You must configure SSL through IIS in Arcon before enabling this option.

CyberArk Vault Options

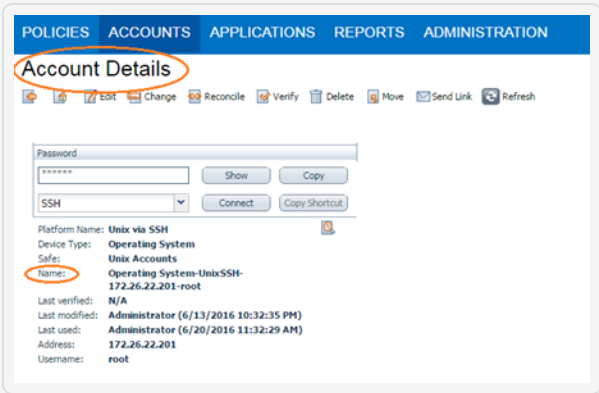
The following table describes the options to configure when using **CyberArk Vault** as the authentication method for Windows credentials.

Option	Description
Username	The username for the target system.



Option	Description
Domain	The domain, if the username is part of a domain.
Central Credential Provider URL Host	The CyberArk Central Credential Provider IP/DNS address.
Central Credential Provider URL Port	The port the CyberArk Central Credential Provider is listening on.
Vault Username	The username for the vault, if the CyberArk Central Credential Provider is configured for basic authentication.
Vault Password	The password for the vault, if the CyberArk Central Credential Provider is configured for basic authentication.
Safe	The safe on the CyberArk Central Credential Provider server that contains the credentials you want to retrieve.
CyberArk Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host.
CyberArk Client Certificate Private Key	The file that contains the PEM private key for the client certificate.
CyberArk Client Certificate Private Key Passphrase	The passphrase for the private key, if required.
AppID	The AppID with CyberArk Central Credential Provider permissions to retrieve the target password.
Folder	The folder on the CyberArk Central Credential Provider server that contains the credentials you want to retrieve.



Option	Description
PolicyID	The PolicyID assigned to the credentials you want to retrieve.
Vault Use SSL	When enabled, Tenable.sc uses SSL through IIS for secure communications. You must configure SSL through IIS in CyberArk Central Credential Provider before enabling this option.
Vault Verify SSL	When enabled, Tenable.sc validates the SSL certificate. You must configure SSL through IIS in CyberArk Central Credential Provider before enabling this option. For more information about using self-signed certificates, see Custom Plugin Packages for NASL and CA Certificate Upload .
CyberArk Escalation Account Details Name	The unique name of the credential you want to retrieve from CyberArk. 
CyberArk AIM Service URL	The URL for the CyberArk AIM web service. By default, Tenable.sc uses /AIMWebservice/v1.1/AIM.asmx.

Hashicorp Vault Options

The following table describes the additional options to configure when using **Hashicorp Vault** as the authentication method for SSH credentials.

Option	Default Value	Required
Hashicorp Host	The Hashicorp Vault IP address or DNS address.	yes



	Note: If your Hashicorp Vault installation is in a sub-directory, you must include the subdirectory path. For example, type <i>IP address or hostname/sub-directory path</i> .	
Hashicorp Port	The port on which Hashicorp Vault listens.	yes
Authenticaton Type	Specifies the authentication type for connecting to the instance: App Role or Certificates. If you select Certificates, additional options for Hashicorp Client Certificate (Required) and Hashicorp Client Certificate Private Key (Required) appear. Select the appropriate files for the client certificate and private key.	yes
Role ID	The GUID provided by Hashicorp Vault when you configured your App Role.	yes
Role Secret ID	The GUID generated by Hashicorp Vault when you configured your App Role.	yes
Authentication URL	The URL used to access Hashicorp Vault.	yes
Namespace	The name of a specified team in a multi-team environment.	no
Hashicorp Vault Type	The type of Hashicorp Vault secrets engine: • KV1 – Key/Value Secrets Engine Version 1 • KV2 – Key/Value Secrets Engine Version 2 • AD – Active Directory	yes
KV Engine URL	The URL Tenable.sc uses to access the Hashicorp Vault secrets engine.	yes
Username Source	(Only displays if Hashicorp Vault Type is KV1 or KV2) Specifies if the username is input manually or pulled from Hashicorp Vault.	yes



Username key	(Only displays if Hashicorp Vault Type is KV1 or KV2) The name in Hashicorp Vault that user-names are stored under.	yes
Password key	(Only displays if Hashicorp Vault Type is KV1 or KV2) The key in Hashicorp Vault that passwords are stored under.	yes
Secret Name	The key secret you want to retrieve values for.	yes
Use SSL	When enabled, Tenable.sc uses SSL for secure communications. You must configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL	When enabled, Tenable.sc validates the SSL certificate. You must configure SSL in Hashicorp Vault before enabling this option.	no

Kerberos Options

The following table describes the options to configure when using **Kerberos** as the authentication method for Windows credentials.

Option	Description
Username	The username for a user on the target system.
Password	The password associated with the username you provided.
Domain	The authentication domain, typically the domain name of the target (e.g., <i>example.com</i>).
KDC Host	The host supplying the session tickets.
KDC Port	The port you want to use for the KDC connection. By default, Tenable.sc uses port 88.
KDC Transport	The method you want to use to connect to the KDC server. Note: If you select UDP, you may need to edit the KDC Port. The KDC UDP pro-



Option	Description
	toocol uses either port 88 or port 750.

LM Hash Options

The following table describes the options to configure when using **LM Hash** as the authentication method for Windows credentials.

Option	Description
Username	The username for a user on the target system.
Hash	The LM hash you want to use.
Domain	The domain of the username, if required.

NTLM Hash Options

The following table describes the options to configure when using **NTLM Hash** as the authentication method for Windows credentials.

Option	Description
Username	The username for a user on the target system.
Hash	The NTLM hash you want to use.
Domain	The domain of the username, if required.

Password Options

The following table describes the options to configure when using **Password** as the authentication method for Windows credentials.

Option	Description
Username	The username for a user on the target system.



Option	Description
Password	The password associated with the username you provided.
Domain	The domain of the username, if required.

Thycotic Secret Server Options

The following table describes the options to configure when using **Thycotic Secret Server** as the authentication method for Windows credentials.

Option	Description
Username	(Required) The username for a user on the target system.
Domain	The domain of the username, if set on the Thycotic server.
Thycotic Secret Name	The Secret Name value on the Thycotic server.
Thycotic Secret Server URL	(Required) The value you want Tenable.sc to use when setting the transfer method, target, and target directory for the scanner. Find the value on the Thycotic server, in Admin > Configuration > Application Settings > Secret Server URL. For example, if you type <i>https://pw.mydomain.com/SecretServer</i>, Tenable.sc determines it is an SSL connection, that <i>pw.mydomain.com</i> is the target address, and that <i>/SecretServer</i> is the root directory.
Thycotic Login Name	(Required) The username for a user on the Thycotic server.
Thycotic Password	(Required) The password associated with the Thycotic Login Name you provided.
Thycotic Organization	In cloud instances of Thycotic, the value that identifies which organization the Tenable.sc query should target.
Thycotic Domain	The domain, if set for the Thycotic server.



Option	Description
Use Private Key	If enabled, Tenable.sc uses key-based authentication for SSH connections instead of password authentication.
Verify SSL Certificate	If enabled, Tenable.sc verifies the SSL Certificate on the Thycotic server. For more information about using self-signed certificates, see Custom Plugin Packages for NASL and CA Certificate Upload .

BeyondTrust Options

The following table describes the options to configure when using **BeyondTrust** as the authentication method for Windows credentials.

Option	Description
Username	The username to log in to the hosts you want to scan.
Domain	The domain of the username, if required by BeyondTrust.
BeyondTrust Host	The BeyondTrust IP address or DNS address.
BeyondTrust Port	The port BeyondTrust is listening on.
BeyondTrust API User	The API user provided by BeyondTrust.
BeyondTrust API Key	The API key provided by BeyondTrust.
Checkout Duration	The length of time, in minutes, that you want to keep credentials checked out in BeyondTrust. Configure the Checkout duration to exceed the typical duration of your Tenable.sc scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. Tip: Configure the password change interval in BeyondTrust so that password changes do not disrupt your Tenable.sc scans. If BeyondTrust changes a password during a scan, the scan fails.



Option	Description
Use SSL	If enabled, Tenable.sc uses SSL through IIS for secure communications. You must configure SSL through IIS in BeyondTrust before enabling this option.
Verify SSL Certificate	If enabled, Tenable.sc validates the SSL certificate. You must configure SSL through IIS in BeyondTrust before enabling this option.

Lieberman Options

The following table describes the additional options to configure when using **Lieberman** as the authentication method for Windows credentials.

Option	Description
Username	The username for a user on the database.
Domain	The domain of the username, if required by Lieberman.
Lieberman Host	The Lieberman IP address or DNS address. Note: If your Lieberman installation is in a subdirectory, you must include the subdirectory path. For example, type <i>IP address or hostname/sub-directory path</i>.
Lieberman Port	The port Lieberman is listening on.
Lieberman User	The username for the Lieberman explicit user you want Tenable.sc to use for authentication to the Lieberman Rapid Enterprise Defense (RED) API.
Lieberman Password	The password for the Lieberman explicit user.
Use SSL	When enabled, Tenable.sc uses SSL through IIS for secure communications. You must configure SSL through IIS in Lieberman before enabling this option.
Verify	When enabled, Tenable.sc validates the SSL certificate. You must con-



Option	Description
SSL Certificate	figure SSL through IIS in Lieberman before enabling this option. For more information about using self-signed certificates, see Custom Plugin Packages for NASL and CA Certificate Upload .
System Name	The name for the database credentials in Lieberman.



Audit Files

The Nessus vulnerability scanner allows you to perform compliance audits of numerous platforms including (but not limited to) databases, Cisco, Unix, and Windows configurations as well as sensitive data discovery based on regex contained in audit files. Audit files are XML-based text files that contain the specific configuration, file permission, and access control tests to be performed. For more information, see [Manage Audit Files](#).

After you create an audit file, you can reference the audit file in a template-based Policy Compliance Auditing scan policy or a custom scan policy. For more information about compliance options in custom scan policies, see [Compliance Options](#).

For more information on compliance checks and creating custom audits, see the [Compliance Checks Reference](#).

Template-Based Audit Files

You can add template-based audit files using templates embedded within Tenable.sc. Tenable updates these templates regularly through the Tenable.sc feed.

For more information, see [Add a Template-Based Audit File](#).

Custom Audit Files

You can add custom audit files to upload any of the following:

- a Tenable-created audit file downloaded from the [Tenable downloads](#) page.
- a Security Content Automation Protocol (SCAP) Data Stream file downloaded from a SCAP repository (e.g., <https://nvd.nist.gov/ncp/repository>).

The file must contain full SCAP content (Open Vulnerability and Assessment Language (OVAL) and Extensible Configuration Checklist Description Format (XCCDF) content) or OVAL standalone content.

Note: XCCDF standalone content audit files lack automated checks and do not return scan results in Tenable.sc.



- a custom audit file created or customized for a specific environment. For more information, see the [knowledge base](#) article.

For more information, see [Add a Custom Audit File](#).



Add a Template-Based Audit File

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

You can add template-based audit files using templates embedded within Tenable.sc. Tenable updates these templates regularly through the Tenable.sc feed.

For more information, see [Audit Files](#).

To add a template-based audit file:

1. Log in to Tenable.sc.
2. Click **Scanning** > **Audit Files** (administrator users) or **Scans** > **Audit Files** (organizational users).

The **Audit Files** page appears.

3. Click **Add**

The **Add Audit File** page appears.

The **Audit File Templates** page appears.

4. In the **TemplatesCommon** section, click a template category tile.

The **Add Audit Template** page appears.

5. In the **Name** box, type a name for the audit file.
6. (Optional) In the **Description** box, type a description for the audit file.
7. (Optional) Edit the template-specific options if you do not want to use the default values.
8. Click **Submit**.

Tenable.sc saves your configuration.

What to do next:



- Reference the audit file in a template-based Policy Compliance Auditing scan policy or a custom scan policy. For more information about compliance options in custom scan policies, see [Compliance Options](#).



Add a Custom Audit File

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

You can add custom audit files to upload any of the following:

- a Tenable-created audit file downloaded from the [Tenable downloads](#) page.
- a Security Content Automation Protocol (SCAP) Data Stream file downloaded from a SCAP repository (e.g., <https://nvd.nist.gov/ncp/repository>).

The file must contain full SCAP content (Open Vulnerability and Assessment Language (OVAL) and Extensible Configuration Checklist Description Format (XCCDF) content) or OVAL standalone content.

Note: XCCDF standalone content audit files lack automated checks and do not return scan results in Tenable.sc.

- a custom audit file created or customized for a specific environment. For more information, see the [knowledge base](#) article.

For more information, see [Audit Files](#).

Before you begin:

- Download or prepare the file you intend to upload.

To add a custom audit file or SCAP Data Stream file:

1. Log in to Tenable.sc via the user interface.
2. Click **Scanning** > **Audit Files** (administrator users) or **Scans** > **Audit Files** (organizational users).

The **Audit Files** page appears.

3. Click **Add**

The **Add Audit File** page appears.

The **Audit File Templates** page appears.



4. In the **CustomOther** 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.sc saves your configuration.

What to do next:

- Reference the audit file in a template-based Policy Compliance Auditing scan policy or a custom scan policy. For more information about compliance options in custom scan policies, see [Compliance Options](#).



Manage Audit Files

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

For more information, see [Audit Files](#).

To manage your audit files:

1. Log in to Tenable.sc via the user interface.
2. Click **Scans > Audit Files**.

The **Audit Files** page appears.

3. To filter the audit files that appear on the page, apply a filter as described in [Apply a Filter](#).
4. To add an audit file, see [Add a Template-Based Audit File](#) or [Add a Custom Audit File](#).

5. To view details for an audit file:

- a. In the row for the audit file, click the  menu.

The actions menu appears.

- b. Click **View**.

The **View Audit File** page appears.

6. To edit or replace an audit file:

- a. In the row for the audit file, click the  menu.

The actions menu appears.

- b. Click **Edit**.

The **Edit Audit File** page appears.

- c. To edit the name or description, type a new **Name** or **Description**.
- d. To replace the audit file, click the delete button (✖) next to the file and upload a new audit file.



- e. Click **Submit**.

Tenable.sc saves your configuration.

7. To share or revoke access to an audit file:

- a. In the row for the audit file, click the  menu.

The actions menu appears.

- b. Click **Share**.
- c. Share or revoke access for each group in your organization.
- d. Click **Submit**.

Tenable.sc saves your configuration.

8. To export an audit file:

- a. In the row for the audit file, click the  menu.

The actions menu appears.

- b. Click **Export**.

Tenable.sc exports the audit file.

9. To delete an audit file:

- a. In the row for the audit file, click the  menu

The actions menu appears..

- b. Click **Delete**.

A confirmation window appears.

- c. Click **Delete**.

Tenable.sc deletes the audit file.



Scan Zones

Scan zones are areas of your network that you want to target in an active scan, associating an IP address or range of IP addresses with one or more scanners in your deployment. You must create scan zones in order to run active scans in Tenable.sc.

For more information, see [Add a Scan Zone](#), [View Your Scan Zones](#), [Edit a Scan Zone](#), and [Delete a Scan Zone](#).

Option	Description
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 Nessus Manager for agent management, do not target Nessus Manager in any scan zone ranges.

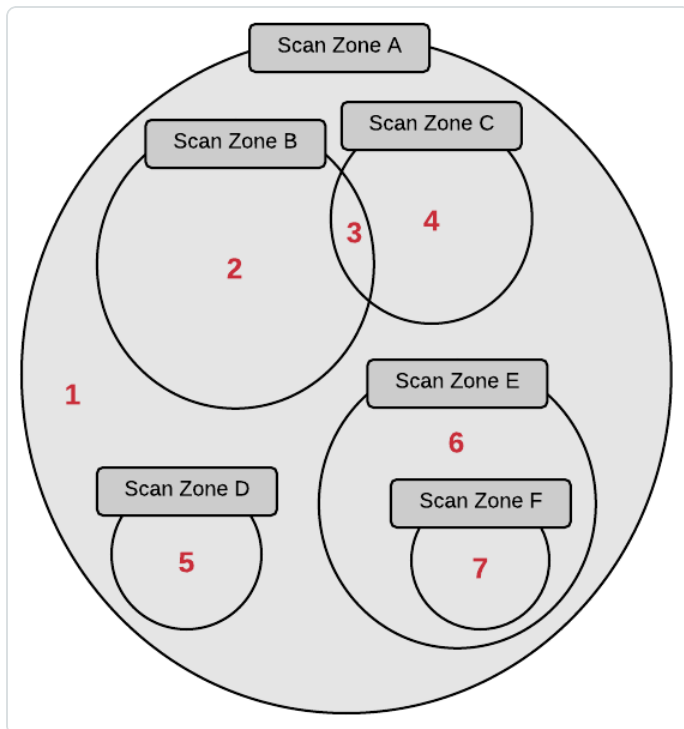
Overlapping Scan Zones

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.sc 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.



Add a Scan Zone

Required User Role: Administrator

For more information about scan zone options, see [Scan Zones](#).

To add a scan zone:

1. Log in to Tenable.sc via the user interface.
2. Click **Resources** > **Scan Zones**.

The **Scan Zones** page appears.

3. Click **Add**.

The **Add Scan Zone** page appears.

4. In the **Name** box, type a name for the scan zone.
5. In the **Description** box, type a description for the scan zone.
6. In the **Ranges** box, type one or more IP addresses, CIDR addresses, or ranges to target with the scan zone.
7. In the **Scanners** box, choose one or more scanners to associate with the scan zone.
8. Click **Submit**.

Tenable.sc saves your configuration.

What to do next:

- Configure scan zone-related organization settings, as described in [Organizations](#).
- Configure an active scan that targets your scan zone, as described in [Add an Active Scan](#).



View Your Scan Zones

Required User Role: Administrator

For more information, see [Scan Zones](#).

To view a list of configured scan zones:

1. Log in to Tenable.sc via the user interface.
2. Click **Resources** > **Scan Zones**.

The **Scan Zones** page appears.

3. View details about each scan zone.
 - **Name** — The name of the scan zone.
 - **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 [Nessus Scanner Statuses](#).

- **Scanners** — The number of Nessus scanners in the scan zone.
- **Last Modified** — The date and time the scan zone was last modified.



Edit a Scan Zone

Required User Role: Administrator

For more information about scan zone options, see [Scan Zones](#).

To edit a scan zone:

1. Log in to Tenable.sc via the user interface.
2. Click **Resources** > **Scan Zones**.

The **Scan Zones** page appears.

3. In the row for the scan zone you want to edit, click the  menu.

The actions menu appears.

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**

6. Click **Submit**.

Tenable.sc saves your configuration.



Delete a Scan Zone

Required User Role: Administrator

For more information, see [Scan Zones](#).

Before you begin:

- Confirm that no scans target the scan zone you want to delete. Tenable.sc scans may fail if you delete an actively targeted scan zone.

To delete a scan zone:

1. Log in to Tenable.sc via the user interface.
2. Click **Resources > Scan Zones**.

The **Scan Zones** page appears.

3. In the row for the scan zone you want to delete, click the  menu.

The actions menu appears.

4. Click **Delete**.

A confirmation window appears.

5. Click **Delete**.

Tenable.sc deletes the scan zone.



Scan Policies

Scan policies contain plugin settings and advanced directives for active scans.

When an administrator user creates a scan policy, the policy is available to all organizations. When an organizational user creates a scan policy, the scan policy is available only to their organization. Users with the appropriate permissions can use scan policies in an active scan, modify policy options, and more. For more information about user permissions, see [User Roles](#).

For more information, see:

- [Add a Scan Policy](#)
- [Scan Policy Templates](#)
- [Scan Policy Options](#)
- [View Your Scan Policies](#)
- [View Scan Policy Details](#)
- [Edit a Scan Policy](#)
- [Share or Revoke Access to a Scan Policy](#)
- [Export a Scan Policy](#)
- [Import a Scan Policy](#)
- [Copy a Scan Policy](#)
- [Delete a Scan Policy](#)



Add a Scan Policy

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

You can create template-based or custom scan policies for your active scans. When you create a custom scan policy, you can configure any scan policy option. When you configure a template-based scan policy, you can configure the options included for the template type.

For more information, see [Scan Policies](#) and [Active Scans](#).

To add a template-based scan policy:

1. Log in to Tenable.sc via the user interface.
2. Click **Scanning > Policies** (administrator users) or **Scans > Policies** (organizational users).

The **Policies** page appears.

3. Click **Add**.

The **Add Policy** page appears.

4. In the **Template** section, click a policy template. For more information, see [Scan Policy Templates](#).

The policy template page appears.

5. Configure the options described in [Scan Policy Options](#).
6. Click **Submit**.

Tenable.sc saves your configuration.

To add a custom scan policy:

1. Log in to Tenable.sc via the user interface.
2. Click **Scanning > Policies** (administrator users) or **Scans > Policies** (organizational users).

The **Policies** page appears.

3. Click **Add**.



The **Add Policy** page appears.

4. In the **Custom** section, click **Advanced Scan**.

The **Advanced Scan** page appears.

5. Configure the options described in [Scan Policy Options](#).
6. Click **Submit**.

Tenable.sc saves your configuration.

What to do next:

- Reference the scan policy in an active scan configuration, as described in [Add an Active Scan](#).



Scan Policy Templates

Tenable.sc provides scan policy templates with pre-configured plugin settings and advanced directives for active scans. You can configure a Tenable-provided template or you can create a fully customized scan policy from all of the available scan policy options in Tenable.sc.

Each Tenable-provided scan policy template contains a different set of scan policy options. You can only modify the settings included for that scan policy template type.

Custom scan policies, such as Advanced Scan, contain all scan policy options. You can modify any scan policy options for custom scans.

For more information, see [Scan Policies](#) and [Scan Policy Options](#).

Template	Description
Template	
Host Discovery	Performs a simple scan to discover live hosts and open ports.
Basic Network Scan	Performs a full system scan that is suitable for any host. For example, you could use this template to perform an internal vulnerability scan on your organization's systems.
Credentialed Patch Audit	Authenticates hosts and enumerates missing updates.
Web Application Tests	Scan for published and unknown web vulnerabilities.
Malware Scan	Scans for malware on Windows and Unix systems.
Policy Compliance Auditing	Audits system configurations against a known baseline.
Internal PCI Network Scan	Performs an internal PCI DSS (11.2.1) vulnerability scan.
SCAP and OVAL Auditing	Audits systems using SCAP and OVAL definitions.



Bash Shellshock Detection	Performs remote and local checks for CVE-2014-6271 and CVE-2014-7169.
GHOST (glibc) Detection	Performs local checks to detect vulnerabilities related to CVE-2015-0235.
PCI Quarterly External Scan	Performs quarterly external scans as required by PCI.
DROWN Detection	Performs remote checks for CVE-2016-0800.
Badlock Detection	Performs remote and local checks for CVE-2016-2118 and CVE-2016-0128.
Intel AMT Security Bypass Detection	Performs remote and local checks for CVE-2017-5689.
WannaCry Ransomware Detection	Scans for the WannaCry ransomware.
Shadow Brokers Scan	Scans for vulnerabilities disclosed in the Shadow Brokers leaks.
Spectre and Melt-down Detection	Performs remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.
Zerologon Remote Scan	Detects Microsoft Netlogon elevation of privilege vulnerability (Zerologon).
Solarigate	Detects SolarWinds Solorigate vulnerabilities using remote and local checks.
2020 Threat Landscape Restrospective (TLR)	Detects vulnerabilities featured in Tenable's 2020 Threat Landscape Retrospective report.
ProxyLogon: MS Exchange	Performs remote and local checks to detect Microsoft Exchange Server vulnerabilities related to CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065.
PrintNightmare	Performs local checks for CVE-2021-34527, the PrintNightmare Windows Print Spooler vulnerability.



Active Directory Starter Scan	Scans for misconfigurations in Active Directory. Note: Active Directory Starter Scans require ADSI credentials. For more information, see Miscellaneous .
Custom	
Advanced Scan	An scan without any recommendations, so that you can fully customize the scan settings.

Template	Description
Common	
Advanced Agent Scan	An agent scan without any recommendations, so that you can fully customize the scan settings.
Advanced Scan	An scan without any recommendations, so that you can fully customize the scan settings.
Basic Network Scan	Performs a full system scan that is suitable for any host. For example, you could use this template to perform an internal vulnerability scan on your organization's systems.
Credentialed Patch Audit	Authenticates hosts and enumerates missing updates.
Web Application Tests	Scan for published and unknown web vulnerabilities.
Compliance Configuration	
Internal PCI Network Scan	Performs an internal PCI DSS (11.2.1) vulnerability scan.
PCI Quarterly External Scan	Performs quarterly external scans as required by PCI.
Policy Compliance Auditing	Audits system configurations against a known baseline.



SCAP and OVAL Auditing	Audits systems using SCAP and OVAL definitions.
Other	
2020 Threat Landscape Restrospective (TLR)	Detects vulnerabilities featured in Tenable's 2020 Threat Landscape Retrospective report.
Active Directory Starter Scan	Scans for misconfigurations in Active Directory. Note: Active Directory Starter Scans require ADSI credentials. For more information, see Miscellaneous.
Badlock Detection	Performs remote and local checks for CVE-2016-2118 and CVE-2016-0128.
Bash Shellshock Detection	Performs remote and local checks for CVE-2014-6271 and CVE-2014-7169.
DROWN Detection	Performs remote checks for CVE-2016-0800.
GHOST (glibc) Detection	Performs local checks to detect vulnerabilities related to CVE-2015-0235.
Host Discovery	Performs a simple scan to discover live hosts and open ports.
Intel AMT Security Bypass Detection	Performs remote and local checks for CVE-2017-5689.
Malware Scan	Scans for malware on Windows and Unix systems.
PrintNightmare	Performs local checks for CVE-2021-34527, the PrintNightmare Windows Print Spooler vulnerability.
ProxyLogon: MS Exchange	Performs remote and local checks to detect Microsoft Exchange Server vulnerabilities related to CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065.
Shadow Brokers Scan	Scans for vulnerabilities disclosed in the Shadow Brokers leaks.
Solarigate	Detects SolarWinds Solorigate vulnerabilities using remote and local



	checks.
Spectre and Melt-down Detection	Performs remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.
WannaCry Ransomware Detection	Scans for the WannaCry ransomware.
Zerologon Remote Scan	Detects Microsoft Netlogon elevation of privilege vulnerability (Zerologon).



Scan Policy Options

Scan policy options specify granular configurations for your active scans.

When you create a custom scan policy, you can configure any scan policy option. When you configure a template-based scan policy, you can configure the options included for the template type.

For more information about Tenable-provided scan policy templates, see [Scan Policy Templates](#).

- [Setup Options](#)
- [Advanced Options](#)
- [Host Discovery Options](#)
- [Port Scanning Options](#)
- [Service Discovery Options](#)
- [Assessment Options](#)
- [Brute Force Options](#)
- [Malware Options](#)
- [SCADA Options](#)
- [Web Applications Options](#)
- [Windows Options](#)
- [Report Options](#)
- [Authentication Options](#)
- [Compliance Options](#)
- [Plugins Options](#)

Setup Options

Option	Description
Name	A unique name for the policy.



Option	Description
Description	(Optional) A description for the policy.
Tag	A tag for the policy. For more information, see Tags .

Advanced Options

Option	Description
General Settings	
Enable safe checks	Nessus attempts to identify remote vulnerabilities by interpreting banner information and attempting to exercise a vulnerability. When Enable safe checks is enabled, the second step is skipped. This is not as reliable as a full probe, but is less likely to negatively impact a targeted system.
Stop scanning hosts that become unresponsive during the scan	During a scan, hosts may become unresponsive after a period of time. Enabling this setting stops scan attempts against hosts that stop sending results.
Automatically accept detected SSH disclaimer prompts	When enabled, if a credentialed scan tries to connect via SSH to a FortiOS host that presents a disclaimer prompt, the scanner provides the necessary text input to accept the disclaimer prompt and continue the scan. When disabled, credentialed scans on hosts that present a disclaimer prompt fail because the scanner cannot connect to the device and accept the disclaimer. The error appears in the plugin output.
Create unique identifier on hosts scanned using credentials	When enabled, creates a file that contains a unique identifier for each host for which the scan has credentials. The plugin creates the file at the following locations: • For Linux hosts, <code>/etc/tenable_tag</code>. • For Windows hosts, the registry at <code>HKLM\SOFTWARE\Tenable\TAG</code>. Tagging hosts with unique identifiers provides more complete scan res-



Option	Description
	ults and ensures Tenable.sc accurately includes or excludes assets toward your license count. For more information about license counts, see License Requirements .
Performance Options	
Slow down the scan when network congestion is detected	When Nessus detects congestion during a scan, it will slow the speed of the scan in an attempt to ease the burden on the affected segment(s).
Use Linux kernel congestion detection	Use Linux kernel congestion detection during the scan to help alleviate system lockups on the Nessus scanner server.
Network timeout (in seconds)	Determines the amount of time, in seconds, to determine if there is an issue communicating over the network.
Max simultaneous checks per host	This setting limits the maximum number of checks a Nessus scanner will perform against a single host at one time. The default value of this option is 5 simultaneous checks per host. Type an integer greater than 0. If you enter 0, enter a negative integer, or delete the value in the field, Tenable.sc does not perform any checks and scans will not complete.
Max simultaneous hosts per scan	This setting limits the maximum number of hosts that a single Nessus scanner will scan at the same time. If the scan is using a zone with multiple scanners, each scanner will accept up to the amount specified in the Max simultaneous hosts per scan option. For example, if the Max simultaneous hosts per scan is set to 5 and there are 5 scanners per zone, each scanner will accept 5 hosts to scan, allowing a total of 25 hosts to be scanned between the 5 scanners. The default value of this option is 30 hosts per scan.
Max number of	Specifies the maximum number of established TCP sessions for a single



Option	Description
concurrent TCP sessions per host	host. This TCP throttling option also controls the number of packets per second the SYN scanner sends, which is 10 times the number of TCP sessions. E.g., if this option is set to 15, the SYN scanner sends 150 packets per second at most. Type an integer between 1-2000. If you leave the box empty or enter 0, Tenable.sc does not enforce a limit.
Max number of concurrent TCP sessions per scan	This setting limits the maximum number of TCP sessions established by any of the active scanners during a scan. Type an integer between 1-2000. If you leave the box empty or enter 0, Tenable.sc does not enforce a limit.
Unix find command Options	
Exclude Filepath	A plain text file containing a list of filepaths to exclude from all plugins that search using the <code>find</code> command on Unix systems. In the file, enter one filepath per line, formatted per patterns allowed by the Unix <code>find</code> command <code>-path</code> argument. For more information, see the <code>find</code> command man page.
Exclude Filesystem	A plain text file containing a list of filesystems to exclude from all plugins that search using the <code>find</code> command on Unix systems. In the file, enter one filesystem per line, using filesystem types supported by the Unix <code>find</code> command <code>-fstype</code> argument. For more information, see the <code>find</code> command man page.
Include Filepath	A plain text file containing a list of filepaths to include from all plugins that search using the <code>find</code> command on Unix systems. In the file, enter one filepath per line, formatted per patterns allowed by the Unix <code>find</code> command <code>-path</code> argument. For more information, see the <code>find</code> command man page.



Option	Description
	Including filepaths increases the locations that are searched by plugins, which extends the duration of the scan. Make your inclusions as specific as possible. Tip: Avoid having the same filepaths in Include Filepath and Exclude Filepath. This conflict may result in the filepath being excluded from the search, though results may vary by operating system.
Debug Settings	
Enumerate launched plugins	Displays a list of plugins that were launched during the scan. You can view the list in scan results under plugin 112154.
Stagger scan start	
Maximum delay (minutes)	(Agent scans only) (Agents 8.2 and later) If set, each agent in the agent group delays starting the scan for a random number of minutes, up to the specified maximum. Staggered starts can reduce the impact of agents that use a shared resource, such as virtual machine CPU. If the maximum delay you set exceeds your scan window, Tenable.sc shortens your maximum delay to ensure that agents begin scanning at least 30 minutes before the scan window closes.

Host Discovery Options

Option	Description
Ping the remote host	When enabled, Nessus attempts to ping the hosts in the scan to determine if the host is alive or not.
General Settings (available when Ping the remote host is enabled)	
Test the local Nessus host	This option allows you to include or exclude the local Nessus host from the scan. This is used when the Nessus host falls within the target network range for the scan.
Use fast net-	When Nessus pings a remote IP address and receives a reply, it performs



Option	Description
work discovery	extra checks to make sure that it is not a transparent proxy or a load balancer that would return noise but no result (some devices answer to every port 1 - 65535 even when there is no service behind the device). Such checks can take some time, especially if the remote host is firewalled. If Use fast network discovery is enabled, Nessus will not perform these checks.
Ping Methods (available when Ping the remote host is enabled)	
ARP	Ping a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.
TCP	Ping a host using TCP.
Destination ports	Destination ports can be configured to use specific ports for TCP ping. This option specifies the list of ports that are checked via TCP ping. Type one of the following: • a single port • a comma-delimited list of ports • built-in For more information about which ports built-in specifies, see the knowledge base article.
ICMP	Ping a host using the Internet Control Message Protocol (ICMP).
Assume ICMP unreachable means the host is down	When a ping is sent to a host that is down, its gateway may return an ICMP unreachable message. When enabled, this option will consider this to mean the host is dead. This is to help speed up discovery on some networks. Note that some firewalls and packet filters use this same behavior for hosts that are up but are connecting to a port or protocol that is filtered. With this option enabled, this will lead to the scan considering the host is down when it is indeed up.



Option	Description
Maximum number of retries (ICMP enable)	Allows you to specify the number of attempts to try to ping the remote host. The default is two attempts.
UDP	Ping a host using the User Datagram Protocol (UDP). Tip: UDP is a stateless protocol, meaning that communication is not performed with handshake dialogues. UDP-based communication is not always reliable, and because of the nature of UDP services and screening devices, they are not always remotely detectable.
Fragile Devices	
Scan Network Printers	Instructs the Nessus scanner not to scan network printers if unselected. Since many printers are prone to denial of service conditions, Nessus can skip scanning them once identified. This is particularly recommended if scanning is performed on production networks.
Scan Novell Netware Hosts	Instructs the Nessus scanner not to scan Novel Netware hosts if unselected. Since many Novell Netware hosts are prone to denial of service conditions, Nessus can skip scanning them once identified. This is particularly recommended if scanning is performed on production networks.
Scan Operational Technology devices	When enabled, Tenable.sc performs a full scan of Operational Technology (OT) devices such as programmable logic controllers (PLCs) and remote terminal units (RTUs) that monitor environmental factors and the activity and state of machinery. When disabled, Tenable.sc uses ICS/SCADA Smart Scanning to cautiously identify OT devices and stops scanning them once they are discovered.
Wake-on-LAN	
List of MAC addresses	Wake on Lan (WOL) packets will be sent to the hosts listed, one on each line, in an attempt to wake the specified host(s) during a scan.
Boot time wait (in minutes)	The number of minutes Nessus will wait to attempt a scan of hosts sent a WOL packet.



Port Scanning Options

Option	Description
Ports	
Consider unscanned ports as closed	If a port is not scanned with a selected port scanner (e.g., out of the range specified), The scanner will consider it closed.
Port scan range	Specifies a keyword (default) or a custom port range that you want the scanner to target. - Type default to instruct the scanners to scan approximately 4,790 commonly used ports. The list of ports can be found in the nessus-services file. - Type all to instruct the scanner to scan all 65,536 ports, including port 0. If the Port scan range is all, Tenable.sc does not mitigate vulnerabilities discovered in the scan. For more information, see Mitigated Vulnerabilities. - Type a custom port range to instruct the scanners to scan the custom range of ports. Type a custom port range as a comma-delimited list of ports or port ranges. For example, 21,23,25,80,110 or 1-1024,8080,9000-9200. Tenable.sc applies the custom range to the protocols you specify in the Local Port Enumerators section. If you want to scan both TCP and UDP, you can specify a split range specific to each protocol. For example, if you want to scan a different range of ports for TCP and UDP in the same policy, type T:1-1024,U:300-500. You can also specify a set of ports to scan for both protocols, as well as individual ranges for each separate protocol. For example, 1-1024,T:1024-65535,U:1025.
Local Port Enumerators	
SSH (netstat)	When enabled, the scanner uses netstat to check for open ports from the



Option	Description
	local machine. It relies on the netstat command being available via an SSH connection to the target. This scan is intended for Linux-based systems and requires authentication credentials.
WMI (netstat)	When enabled, the scanner uses netstat to determine open ports while performing a WMI-based scan. In addition, the scanner: • Ignores any custom range specified in the Port Scan Range setting. • Continues to treat unscanned ports as closed if the Consider unscanned ports as closed setting is enabled. If any port enumerator (netstat or SNMP) is successful, the port range becomes <i>all</i>.
SNMP	When enabled, if the appropriate credentials are provided by the user, the scanner can better test the remote host and produce more detailed audit results. For example, there are many Cisco router checks that determine the vulnerabilities present by examining the version of the returned SNMP string. This information is necessary for these audits.
Only run network port scanners if local port enumeration failed	When enabled, the scanner relies on local port enumeration first before relying on network port scans.
Verify open TCP ports found by local port enumerators	When enabled, if a local port enumerator (for example, WMI or netstat) finds a port, the scanner also verifies that the port is open remotely. This approach helps determine if some form of access control is being used (for example, TCP wrappers or a firewall).
Network Port Scanners	
TCP	Use the built-in Nessus TCP scanner to identify open TCP ports on the tar-



Option	Description
	gets, using a full TCP three-way handshake. TCP scans are only possible if you are using Linux or FreeBSD. On Windows or Mac OS X, the scanner does not do a TCP scan and instead uses the SYN scanner to avoid performance issues native to those operating systems. If you enable this option, you can also set the Override Automatic Firewall Detection option. Note: On some platforms (e.g., Windows and Mac OS X), if the operating system is causing serious performance issues using the TCP scanner, Nessus will launch the SYN scanner instead.
SYN	Use the built-in Nessus SYN scanner to identify open TCP ports on the target hosts. SYN scans do not initiate a full TCP three-way handshake. The scanner sends a SYN packet to the port, waits for SYN-ACK reply, and determines the port state based on a response or lack of response. If you enable this option, you can also set the Override Automatic Firewall Detection option.
Override automatic firewall detection	Rely on local port enumeration first before relying on network port scans.
UDP	This option engages the built-in Nessus UDP scanner to identify open UDP ports on the targets. Due to the nature of the protocol, it is generally not possible for a port scanner to tell the difference between open and filtered UDP ports. Enabling the UDP port scanner may dramatically increase the scan time and produce unreliable results. Consider using the netstat or SNMP port enumeration options instead if possible.

Service Discovery Options

The **Service Discovery** tab specifies how the scanner looks for services running on the target's ports.



Option	Description
Probe all ports to find services	When enabled, the scanner attempts to map each open port with the service that is running on that port. Caution: In some rare cases, probing might disrupt some services and cause unforeseen side effects.
Search for SSL/TLS services	Controls how the scanner tests SSL-based services. Caution: Testing for SSL capability on all ports may be disruptive for the tested host.
Search for SSL/TLS on	Specifies which ports on target hosts the scanner searches for SSL/TLS services. This setting has two options: • Known SSL/TLS ports • All ports
Identify certificates expiring within x days	Identifies SSL certificates that will expire within the specified timeframe. Type a value to set a timeframe (in days).
Enumerate all SSL/TLS ciphers	When Tenable.sc performs an SSL scan, it tries to determine the SSL ciphers used by the remote server by attempting to establish a connection with each different documented SSL cipher, regardless of what the server says is available.
Enable CRL checking (connects to the Internet)	Direct Nessus to check SSL certificates against known Certificate Revocation Lists (CRL). Enabling this option will make a connection and query one or more servers on the internet.

Assessment Options

The **Assessment** tab specifies how the scanner tests for information during the scan.



Value	Description
Accuracy	
Override normal accuracy	In some cases, Nessus cannot remotely determine whether a flaw is present or not. If report paranoia is set to Paranoid then a flaw will be reported every time, even when there is a doubt about the remote host being affected. Conversely, a paranoia setting of Avoid false alarms will cause Nessus to not report any flaw whenever there is a hint of uncertainty about the remote host. Normal is a middle ground between these two settings.
Perform thorough tests (may disrupt your network or impact scan speed)	Causes various plugins to use more aggressive settings. For example, when looking through SMB file shares, a plugin can analyze 3 directory levels deep instead of its default of 1. This could cause much more network traffic and analysis in some cases. Note that by being more thorough, the scan will be more intrusive and is more likely to disrupt the network, while potentially providing better audit results.
Antivirus	
Antivirus definition grace period (in days)	This option determines the delay in the number of days of reporting the software as being outdated. The valid values are between 0 (no delay, default) and 7.
SMTP	
Third party domain	Nessus attempts to send spam through each SMTP device to the address listed in this option. This third party domain address must be outside the range of the site being scanned or the site performing the scan. Otherwise, the test may be aborted by the SMTP server.
From address	The test messages sent to the SMTP server(s) will appear as if they originated from the address specified in this option.
To Address	Nessus attempts to send messages addressed to the mail recipient listed in this option. The postmaster address is the default value since it is a valid address on most mail servers.



Brute Force Options

The **Brute Force** tab specifies how the scanner tests for information against SCADA systems.

Additionally, if Hydra is installed on the same host as a Nessus server linked to Tenable.sc, the Hydra section is enabled. Hydra extends brute force login testing for the following services: Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, S7-300, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP, SOCKS5, SSH (v1 and v2), Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP.

Option	Description
General Settings	
Only use credentials provided by the user	In some cases, Nessus can test default accounts and known default passwords. This can cause the account to be locked out if too many consecutive invalid attempts trigger security protocols on the operating system or application. By default, this setting is enabled to prevent Nessus from performing these tests.
Oracle Database	
Test default Oracle accounts (slow)	Test for known default accounts in Oracle software.
Hydra	
Always enable Hydra (slow)	Enables Hydra whenever the scan is performed.
Logins file	A file that contains user names that Hydra will use during the scan.
Passwords file	A file that contains passwords for user accounts that Hydra will use during the scan.



Option	Description
Number of parallel tasks	The number of simultaneous Hydra tests that you want to execute. By default, this value is 16.
Timeout (in seconds)	The number of seconds per login attempt.
Try empty passwords	If enabled, Hydra will additionally try user names without using a password.
Try login as password	If enabled, Hydra will additionally try a user name as the corresponding password.
Stop brute forcing after the first success	If enabled, Hydra will stop brute forcing user accounts after the first time an account is successfully accessed.
Add accounts found by other plugins to the login file	If disabled, only the user names specified in the logins file will be used for the scan. Otherwise, additional user names discovered by other plugins will be added to the logins file and used for the scan.
PostgreSQL database name	The database that you want Hydra to test.
SAP R3 Client ID (0 - 99)	The ID of the SAP R3 client that you want Hydra to test.
Windows accounts to test	Can be set to Local accounts , Domain Accounts , or Either .
Interpret passwords as NTLM hashes	If enabled, Hydra will interpret passwords as NTLM hashes.
Cisco login password	This password is used to login to a Cisco system before brute forcing enable passwords. If no password is provided here, Hydra will attempt to login



Option	Description
	using credentials that were successfully brute forced earlier in the scan.
Web page to brute force	Type a web page that is protected by HTTP basic or digest authentication. If a web page is not provided here, Hydra will attempt to brute force a page discovered by the Nessus web crawler that requires HTTP authentication.
HTTP proxy test website	If Hydra successfully brute forces an HTTP proxy, it will attempt to access the website provided here via the brute forced proxy.
LDAP DN	The LDAP Distinguish Name scope that Hydra will authenticate against.

Malware Options

The **Malware** tab specifies options for DNS Resolution, hash, and whitelist files and file system scanning.

Option	Description
Malware Scan Settings	
Malware scan	When enabled, displays the General Settings , Hash and Whitelist Files , and File System Scanning sections.
General Settings (available when Malware scan is enabled)	
Disable DNS Resolution	Checking this option will prevent Nessus from using the cloud to compare scan findings against known malware.
Hash and Whitelist Files (available when Malware scan is enabled)	
Custom Netstat IP Threat List	A text file that contains a list of known bad IP addresses that you want to detect. Each line in the file must begin with an IPv4 address. Optionally, you can add a description by adding a comma after the IP address, followed by the description. You can also use hash-delimited comments (e.g., #) in addition to comma-delimited comments. Note: Tenable does not detect private IP ranges in the text file.



Provide your own list of known bad MD5/SHA1/SHA256 hashes	Additional known bad MD5 hashes can be uploaded via a text file that contains one MD5 hash per line. If you want to add a description for each hash, type a comma after the hash, followed by the description. If any matches are found when scanning a target and a description was provided for the hash, the description will show up in the scan results.
Provide your own list of known good MD5/SHA1/SHA256 hashes	Additional known good MD5 hashes can be uploaded via a text file that contains one MD5 hash per line. If you want to add a description for each hash, type a comma after the hash, followed by the description. If any matches are found when scanning a target and a description was provided for the hash, the description will show up in the scan results.
Hosts file whitelist	Nessus checks system hosts files for signs of a compromise (e.g., Plugin ID 23910). This option allows you to upload a file containing a list of IPs and hostnames that will be ignored by Nessus during a scan. Include one IP address and hostname (formatted identically to your hosts file on the target) per line in a regular text file.
File System Scanning (available when Malware scan is enabled)	
Scan File System	Turning on this option allows you to scan system directories and files on host computers. Caution: Enabling this setting in scans targeting 10 or more hosts could result in performance degradation.
Directories (available when File System Scanning is enabled)	
Scan %Systemroot%	Enable file system scanning to scan %Systemroot%.
Scan %ProgramFiles%	Enable file system scanning to scan %ProgramFiles%.
Scan %ProgramFiles(x86)%	Enable file system scanning to scan %ProgramFiles(x86)%.



(x86)%	
Scan %ProgramData%	Enable file system scanning to scan %ProgramData%.
Scan User Profiles	Enable file system scanning to scan user profiles.
Custom Filescan Directories	A custom file that lists directories for malware file scanning. List each directory on one line. Caution: Root directories such as C:\ or D:\ are not accepted.
Yara Rules Files	A .yar file containing the YARA rules to be applied in the scan. You can only upload one file per scan, so include all rules in a single file. For more information, see yara.readthedocs.io .

SCADA Options

The **SCADA** tab specifies how the scanner tests for information against SCADA systems.

Option	Description
Modbus/TCP Coil Access	
Start at register End at register	These options are available for commercial users. This drop-down box item is dynamically generated by the SCADA plugins available with the commercial version of Nessus. Modbus uses a function code of 1 to read coils in a Modbus slave. Coils represent binary output settings and are typically mapped to actuators. The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a write coil message. The defaults for this are 0 for the Start at register value and 16 for the End at register value.
ICCP/COTP TSAP Addressing Weakness	
Start COTP TSAP Stop COTP TSAP	The ICCP/COTP TSAP Addressing menu determines a Connection Oriented Transport Protocol (COTP) Transport Service Access Points (TSAP) value on an ICCP server by trying possible values. The start and stop values are set to 8 by default.



Web Applications Options

The **Web Applications** tab specifies how the scanner tests for information against web server applications.

Value	Description
Web Application Settings	
Scan web applications	When enabled, displays the General Settings , Web Crawler , and Application Test Settings sections.
General Settings (available when Scan web applications is enabled)	
Use a custom User-Agent	Specifies which type of web browser Nessus will impersonate while scanning.
Web Crawler (available when Scan web applications is enabled)	
Start crawling from	The URL of the first page that will be tested. If multiple pages are required, use a colon delimiter to separate them (e.g., <code>/:/php4:/base</code>).
Excluded pages (regex)	Enable exclusion of portions of the web site from being crawled. For example, to exclude the <code>/manual</code> directory and all Perl CGI, set this option to: <code>(^/manual)(\..pl(?:.*)?\$/)</code> . Nessus supports POSIX regular expressions for string matching and handling, as well as Perl-compatible regular expressions (PCRE).
Maximum pages to crawl	The maximum number of pages to crawl.
Maximum depth to crawl	Limit the number of links Nessus will follow for each start page.
Follow dynamically generated pages	If selected, Nessus will follow dynamic links and may exceed the parameters set above.
Application Test Settings (available when Scan web applications is enabled)	
Enable generic	Enables the options listed below.



Value	Description
web application tests	
Abort web application tests if HTTP login fails	If Nessus cannot login to the target via HTTP, then do not run any web application tests.
Try all HTTP Methods	This option will instruct Nessus to also use POST requests for enhanced web form testing. By default, the web application tests will only use GET requests, unless this option is enabled. Generally, more complex applications use the POST method when a user submits data to the application. This setting provides more thorough testing, but may considerably increase the time required. When selected, Nessus will test each script/variable with both GET and POST requests. This setting provides more thorough testing, but may considerably increase the time required.
Attempt HTTP Parameter Pollution	When performing web application tests, attempt to bypass filtering mechanisms by injecting content into a variable while supplying the same variable with valid content as well. For example, a normal SQL injection test may look like <code>/target.cgi?a='&b=2</code> . With HTTP Parameter Pollution (HPP) enabled, the request may look like <code>/target.cgi?a='&a=1&b=2</code> .
Test embedded web servers	Embedded web servers are often static and contain no customizable CGI scripts. In addition, embedded web servers may be prone to crash or become non-responsive when scanned. Tenable recommends scanning embedded web servers separately from other web servers using this option.
Test more than one parameter at a time per form	This option manages the combination of argument values used in the HTTP requests. The default, without checking this option, is testing one parameter at a time with an attack string, without trying non-attack variations for additional parameters. For example, Nessus attempts <code>/test.php?arg1=XSS&b=1&c=1</code> where <i>b</i> and <i>c</i> allows other values, without testing each combination. This is the quickest method of testing with the smallest result



Value	Description
	set generated. This drop-down box has five selections: • One value — This tests one parameter at a time with an attack string, without trying non-attack variations for additional parameters. For example, Nessus attempts <code>/test.php?arg1=XSS&b=1&c=1</code> where <i>b</i> and <i>c</i> allows other values, without testing each combination. This is the quickest method of testing with the smallest result set generated. • Some pairs — This form of testing will randomly check a combination of random pairs of parameters. This is the fastest way to test multiple parameters. • All pairs (slower but efficient) — This form of testing is slightly slower but more efficient than the one value test. While testing multiple parameters, it will test an attack string, variations for a single variable and then use the first value for all other variables. For example, Nessus attempts <code>/test.php?arg1=XSS&b=1&c=1</code> and then cycles through the variables so that one is given the attack string, one is cycled through all possible values (as discovered during the mirror process) and any other variables are given the first value. In this case, Nessus will never test for <code>/test.php?a=XSS&b=3&c=3&d=3</code> when the first value of each variable is 1. • Some combinations — This form of testing will randomly check a combination of three or more parameters. This is more thorough than testing only pairs of parameters. Note that increasing the amount of combinations by three or more increases the web application test time. • All combinations (extremely slow) — This method of testing will do a fully exhaustive test of all possible combinations of attack strings with valid input to variables. Where All-pairs testing seeks to create a smaller data set as a tradeoff for speed, all combinations makes no



Value	Description
	compromise on time and uses a complete data set of tests. This testing method may take a long time to complete.
Do not stop after the first flaw is found per web page	This option determines when a new flaw is targeted. This applies at the script level; finding an XSS flaw will not disable searching for SQL injection or header injection, but you will have at most one report for each type on a given port, unless thorough tests is set. Note that several flaws of the same type (e.g., XSS, SQLi, etc.) may be reported sometimes, if they were caught by the same attack. The drop-down has four options: • Per CGI — As soon as a flaw is found on a CGI by a script, Nessus switches to the next known CGI on the same server, or if there is no other CGI, to the next port/server. This is the default option. • Per port (faster) — As soon as a flaw is found on a web server by a script, Nessus stops and switches to another web server on a different port. • Per parameter (slow) — As soon as one type of flaw is found in a parameter of a CGI (e.g., XSS), Nessus switches to the next parameter of the same CGI, or the next known CGI, or to the next port/server. • Look for all flaws (slower) — Perform extensive tests regardless of flaws found. This option can produce a very verbose report and is not recommend in most cases.
URL for Remote File Inclusion	During Remote File Inclusion (RFI) testing, this option specifies a file on a remote host to use for tests. By default, Nessus will use a safe file hosted by Tenable for RFI testing. If the scanner cannot reach the Internet, using an internally hosted file is recommended for more accurate RFI testing.
Maximum run time (minutes)	This option manages the amount of time in minutes spent performing web application tests. This option defaults to 60 minutes and applies to all ports and CGIs for a given web site. Scanning the local network for web sites with small applications will typically complete in under an hour, however web sites with large applications may require a higher value.



Windows Options

The **Windows** tab specifies basic Windows SMB domain options.

Option	Description
General Settings	
Request information about the SMB Domain	When enabled, Nessus queries domain users instead of local users.
User Enumeration Methods	
SAM Registry	When enabled, Nessus enumerates users via the Security Account Manager (SAM) registry.
ADSI Query	When enabled, Nessus enumerates users via Active Directory Service Interfaces (ADSI). To use ADSI, you must also configure ADSI authentication options.
WMI Query	When enabled, Nessus enumerates users via Windows Management Interface (WMI).
RID Brute Forcing	When enabled, Nessus enumerates users via relative identifier (RID) brute forcing. Enabling this setting enables the Enumerate Domain User and Enumerate Local User options.
Enumerate Domain Users (available when RID Brute Forcing is enabled)	
Start UID	1000
End UID	1200
Enumerate Local Users (available when RID Brute Forcing is enabled)	
Start UID	1000
End UID	1200

Report Options

The **Report** tab specifies information to include in the scan's report.



Option	Description
Processing	
Override normal verbosity	Determines the verbosity of the detail in the output of the scan results: • Normal — Provides the standard level of plugin activity in the report. • Quiet — Provides less information about plugin activity in the report to minimize impact on disk space. • Verbose — Provides more information about plugin activity in the report. When this option is selected, the output includes the informational plugins 56310, 64582, and 58651.
Show missing patches that have been superseded	Show patches in the report that have not been applied but have been superseded by a newer patch if enabled.
Hide results from plugins initiated as a dependency	If a plugin is only run due to it being a dependency of a selected plugin, hide the results if enabled.
Output	
Designate hosts by their DNS name	When possible, designate hosts by their DNS name rather than IP address in the reports.
Display hosts that respond to ping	When enabled, show a list of hosts that respond to pings sent as part of the scan.
Display unreachable hosts	Display a list of hosts within the scan range that were not able to be reached during the scan, if enabled.
Display Unicode characters	When enabled, Unicode characters appear in plugin output such as user-names, installed application names, and SSL certificate information. Note: Plugin output may sometimes incorrectly parse or truncate strings with Unicode characters. If this issue causes problems with regular expressions in plugins or custom audits, disable this setting and scan again.



Option	Description
Generate SCAP XML Results	Generate a SCAP XML results file as a part of the report output for the scan.

Authentication Options

The **Authentication** tab specifies authentication options during a scan.

Option	Description
Authentication	
Type	Specifies the type of authentication you want scanners to use for credentialed access to scan targets. Credentialed access gathers more complete data about a target. • Host • Database Credentials • Miscellaneous • Plaintext Authentication • Patch Management
SNMP	
UDP Port Additional UDP port #1 Additional UDP port #2 Additional UDP port #3	This is the UDP port that will be used when performing certain SNMP scans. Up to four different ports may be configured, with the default port being 161.
SSH	
known_hosts file	If an SSH known_hosts file is provided for the scan policy, Nessus will



Option	Description
	only attempt to log in to hosts defined in this file. This helps to ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a login to a system that may not be under your control.
Preferred port	This option is set to direct the scan to connect to a specific port if SSH is known to be listening on a port other than the default of 22.
Client Version	Specifies which type of SSH client to impersonate while performing scans.
Attempt least privilege (experimental)	Enables or disables dynamic privilege escalation. When enabled, if the scan target credentials include privilege escalation, Nessus first attempts to run commands without privilege escalation. If running commands without privilege escalation fails, Nessus retries the commands with privilege escalation. Plugins 102095 and 102094 report whether plugins ran with or without privilege escalation. Note: Enabling this option may increase the time required to perform scans by up to 30%.
Windows	
Never send credentials in the clear	By default, Windows credentials are not sent to the target host in the clear.
Do not use NTLMv1 authentication	When disabled, it is theoretically possible to trick Nessus into attempting to log in to a Windows server with domain credentials via the NTLM version 1 protocol. This provides the remote attacker with the ability to use a hash obtained from Nessus. This hash can be potentially cracked to reveal a username or password. It may also be used to directly log in to other servers. Because NTLMv1 is an insecure protocol, this option is enabled by



Option	Description
	default.
Start the Remote Registry service during the scan	This option tells Nessus to start the Remote Registry service on computers being scanned if it is not running. This service must be running in order for Nessus to execute some Windows local check plugins.
Enable administrative shares during the scan	This option will allow Nessus to access certain registry entries that can be read with administrator privileges.
Start the Server service during the scan	When enabled, the scanner temporarily enables the Windows Server service, which allows the computer to share files and other devices on a network. The service is disabled after the scan completes. By default, Windows systems have the Windows Server service enabled, which means you do not need to enable this setting. However, if you disable the Windows Server service in your environment, and want to scan using SMB credentials, you must enable this setting so that the scanner can access files remotely.
Plaintext Authentication	
Perform patch audits over telnet	When enabled, Tenable.sc uses telnet to connect to the host device for patch audits. Note: This protocol is sent in cleartext and could contain unencrypted usernames and passwords.
Perform patch audits over rsh	When enabled, Tenable.sc permits patch audits over a rsh connection. Note: This protocol is sent in cleartext and could contain unencrypted usernames and passwords.
Perform patch audits over rexec	When enabled, Tenable.sc permits patch audits over a rexec connection. Note: This protocol is sent in cleartext and could contain unencrypted usernames and passwords.



Option	Description
HTTP	
Login method	Specify whether the login action is performed via a GET or POST request.
Re-authenticate delay (seconds)	The delay between authentication attempts, in seconds. Tip: A time delay can help prevent triggering brute force lockout mechanisms.
Follow 30x redirections (# of levels)	If a 30x redirect code is received from a web server, this directs Nessus to follow the link provided or not.
Invert authenticated regex	The regex pattern you want Tenable.sc to look for on the login page that, if found, denies authentication. Tip: Tenable.sc can attempt to match a given string, such as Authentication failed.
Use authenticated regex on HTTP headers	When enabled, Tenable.sc searches the HTTP response headers for a given regex pattern instead of searching the body of a response to better determine authentication state.
Case insensitive authenticated regex	When enabled, Tenable.sc ignores case in regex.

Compliance Options

The **Compliance** tab specifies compliance the audit files to reference in a scan policy. The options available depend on the type of audit file selected.

For more information, see [Audit Files](#) and [Configure Compliance Options](#).

Plugins Options

The **Plugins** tab specifies which plugins are used during the policy's Nessus scan. You can enable or disable plugins in the plugin family view or in the plugin view for more granular control.

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



Caution: The Denial of Service plugin family contains plugins that could cause outages on network hosts if the **Safe Checks** option is not enabled, but it also contains useful checks that do not cause any harm. The Denial of Service plugin family can be used in conjunction with **Safe Checks** to ensure that any potentially dangerous plugins are not run. However, Tenable does not recommend enabling the Denial of Service plugin family in production environments.



Configure Compliance Options

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

You can configure compliance options within a scan policy to reference one or more audit files in a template-based **Policy Compliance Auditing** scan policy or a custom scan policy.

For more information, see [Audit Files](#), [Scan Policies](#), and [Scan Policy Options](#).

To configure compliance options for a scan policy:

1. Begin configuring a scan policy, as described in [Add a Scan Policy](#).

2. In the left navigation bar, click **Compliance**.

The **Compliance** options appear.

3. Click **+ Add Audit File**.

The **Select a Type** drop-down box appears.

4. In the **Select a Type** drop-down box, select the type of audit file you want to reference in the scan policy.

The **Select an Audit File** drop-down box appears.

5. In the **Select an Audit File** drop-down box, select the name of the audit file you want to reference in the scan policy.

6. Click the  button.

Tenable.sc applies the audit file to the scan policy.

7. If required, configure additional options for the audit file you applied to the scan policy. For more information, see [Compliance Options](#).



Configure Plugin Options

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

You can configure plugin options within a scan policy to enable or disable plugins at the plugin family level or individual plugin level.

Note: When Tenable adds new plugins to Tenable.sc, the new plugins are automatically enabled if the entire plugin family they belong to is enabled in your scan policy template. If you only enabled some plugins from a family, you must manually enable new plugins to include them in your scan policy.

To configure plugin options at the plugin family level:

1. Begin configuring a scan, policy as described in [Add a Scan Policy](#).
2. In the left navigation bar, click **Plugins**.

The **Plugins** page appears with the plugin family view displayed.

3. In the **Status** column, view the plugin family status and the number of enabled plugins within the plugin family:
 - **Enabled** — All plugins in the family are enabled. The scan will target the parameters in the plugins.
 - **Disabled** — All plugins in the family are disabled. The scan will not target the parameters in the plugins.

Note: Disabling a plugin family reduces the time and resources required to run the scan.

- **Mixed** — The plugin family contains a combination of **Enabled** and **Disabled** plugins.
4. In the **Total** column, view the number of plugins in the family.
 5. To enable or disable all plugins in the family, click the **Status** box.
 6. To filter the plugin families listed on the page, use the **Select a Filter** drop-down box to build and apply a filter.

The **Total** column becomes the **Matched** column and indicates the number of plugins in the family that match the current filter.



7. To hide all disabled plugin families, click **Hide Disabled**.
8. If you hid all disabled plugin families and you want to show them again, click **Show All**.
9. To sort the plugin families listed on the page, click the **Status**, **Plugin Family**, or **Total** column title.
10. To perform a bulk action on all of the plugin families displayed on the page, click **Enable Shown** or **Disable Shown**.

Tenable.sc enables or disables all plugins within the plugin families shown on the page, not just the number of plugins in the **Total** or **Matched** column. For more granular control, set plugin statuses in the plugin view.

11. To enable or disable individual plugins within a family, click the plugin family name to access the plugin view.

The plugin view appears.

To configure plugin options at the individual plugin level:

1. Begin configuring a scan policy as described in [Add a Scan Policy](#).
2. Click **Plugins** in the left navigation bar.

The **Plugins** page appears.

3. Click the plugin family name.

The plugin view appears.

4. In the **Status** column, view the plugin status:
 - **Enabled** — The plugin is enabled. The scan targets the parameters in the plugins.
 - **Disabled** — The plugin is disabled. The scan does not target the parameters in the plugins.

Disabling a plugin family reduces the time and resources required to run the scan.

5. In the **Plugin ID** column, click the information icon to display the plugin details.
6. To enable or disable a plugin, click the **Status** box.



7. To filter the plugins listed on the page, use the **Select a Filter** drop-down box to build and apply a filter.
8. To hide all disabled plugins, click **Hide Disabled**.
9. If you hid all disabled plugins and you want to show them again, click **Show All**.
10. To sort the plugins listed on the page, click the **Status**, **Plugin Name**, or **Plugin ID** column title.
11. To perform a bulk action on all of the plugins displayed on the page, click **Enable Shown** or **Disable Shown**.

Tenable.sc enables or disables all plugins shown on the page.

12. To return to the plugin family view, click the **Back** option.
13. To view the plugins in a different family, click the drop-down box and select a different plugin family.



Host

Tenable.sc can use SNMPv3 credentials to scan remote systems that use an encrypted network management protocol (including network devices). Tenable.sc uses these credentials to scan for patch auditing or compliance checks.

You can configure SNMPv3 options in scan policies, as described in [Authentication Options](#) and [Add a Scan Policy](#).

SNMPv3 Options

Option	Description	Default
Username	The username for the SNMPv3 account that Tenable.sc uses to perform checks on the target system.	-
Port	(Required) The TCP port that SNMPv3 listens on for communications from Tenable.sc.	161
Security Level	The security level for SNMP: • No authentication and no privacy • Authentication without privacy • Authentication and privacy	Authentication and privacy
Authentication algorithm	The algorithm the remote service supports: MD5 or SHA1 .	SHA1
Authentication password	The password associated with the Username .	-
Privacy algorithm	The encryption algorithm to use for SNMP traffic: AES or DES .	AES
Privacy password	A password used to protect encrypted SNMP communication.	-



Miscellaneous

Tenable.sc supports the following additional authentication methods:

- [ADSI](#)
- [F5](#)
- [IBM iSeries](#)
- [Red Hat Enterprise Virtualization \(RHEV\)](#)
- [Netapp API](#)
- [Palo Alto Networks PAN-OS](#)
- [VMware ESX SOAP API](#)
- [VMware Center SOAP API](#)
- [X.509](#)

You can configure these authentication methods in scan policies, as described in [Authentication Options](#) and [Add a Scan Policy](#).

ADSI

ADSI allows Tenable.sc to query an ActiveSync server to determine if any Android or iOS-based devices are connected. Using the credentials and server information, Tenable.sc authenticates to the domain controller (not the Exchange server) to directly query it for device information. These settings are required for mobile device scanning and Active Directory Starter Scans.

Tenable.sc supports obtaining the mobile information from Exchange Server 2010 and 2013 only.

Option	Description	Default
Domain Controller	(Required) The name of the domain controller for ActiveSync.	-
Domain	(Required) The name of the Windows domain for ActiveSync.	-



Option	Description	Default
Domain Admin	(Required) The domain administrator's username.	-
Domain Password	(Required) The domain administrator's password.	-

F5

Option	Description	Default
Username	(Required) The username for the scanning F5 account that Tenable.sc uses to perform checks on the target system.	-
Password	(Required) The password for the F5 user.	-
Port	(Required) The TCP port that F5 listens on for communications from Tenable.sc.	443
HTTPS	When enabled, Tenable.sc connects using secure communication (HTTPS). When disabled, Tenable.sc connects using standard HTTP.	enabled
Verify SSL Certificate	When enabled, Tenable.sc verifies that the SSL certificate on the server is signed by a trusted CA. Tip: If you are using a self-signed certificate, disable this setting.	enabled

IBM iSeries

Option	Description	Default
Username	(Required) The username for the IBM iSeries account that Tenable.sc uses to perform checks on the target system.	-
Password	(Required) The password for the IBM iSeries user.	-

Red Hat Enterprise Virtualization (RHEV)



Option	Description	Default
Username	(Required) The username for RHEV account that Tenable.sc uses to perform checks on the target system.	-
Password	(Required) The password for the RHEV user.	-
Port	(Required) The TCP port that the RHEV server listens on for communications from Tenable.sc.	443
Verify SSL Certificate	When enabled, Tenable.sc verifies that the SSL certificate on the server is signed by a trusted CA. Tip: If you are using a self-signed certificate, disable this setting.	enabled

Netapp API

Option	Description	Default
Username	(Required) The username for the Netapp API account with HTTPS access that Tenable.sc uses to perform checks on the target system.	-
Password	(Required) The password for the Netapp API user.	-
vFiler	The vFiler nodes to scan for on the target systems. To limit the audit to a single vFiler, type the name of the vFiler. To audit for all discovered Netapp virtual filers (vFilers) on target systems, leave the field blank.	-
Port	(Required) The TCP port that Netapp API listens on for communications from Tenable.sc.	443

Palo Alto Networks PAN-OS

Option	Description	Default
Username	(Required) The username for the PAN-OS account that Ten-	-



	able.sc uses to perform checks on the target system.	
Password	(Required) The password for the PAN-OS user.	-
Port	(Required) The TCP port that PAN-OS listens on for communications from Tenable.sc.	443
Verify SSL Certificate	When enabled, Tenable.sc verifies that the SSL certificate on the server is signed by a trusted CA. Tip: If you are using a self-signed certificate, disable this setting.	enabled

VMware ESX SOAP API

Tenable.sc can access VMware servers through the native VMware SOAP API.

Option	Description	Default
Username	(Required) The username for the ESXi server account that Tenable.sc uses to perform checks on the target system.	-
Password	(Required) The password for the ESXi user.	-
Do not verify SSL Certificate	Do not validate the SSL certificate for the ESXi server.	disabled

VMware Center SOAP API

Tenable.sc can access vCenter through the native VMware vCenter SOAP API. If available, Tenable.sc uses the vCenter REST API to collect data in addition to the SOAP API.

Note: You must use a vCenter admin account with read and write permissions.

Option	Description	Default
vCenter Host	(Required) The name of the vCenter host.	-
vCenter Port	(Required) The TCP port that vCenter listens on for communications from Tenable.sc.	443



Option	Description	Default
Username	(Required) The username for the vCenter server account with admin read/write access that Tenable.sc uses to perform checks on the target system.	-
Password	(Required) The password for the vCenter server user.	-
HTTPS	When enabled, Tenable.sc connects using secure communication (HTTPS). When disabled, Tenable.sc connects using standard HTTP.	enabled
Verify SSL Certificate	When enabled, Tenable.sc verifies that the SSL certificate on the server is signed by a trusted CA. Tip: If you are using a self-signed certificate, disable this setting.	enabled

X.509

Option	Description	Default
Client Certificate	(Required) The client certificate.	-
Client Key	(Required) The client private key.	-
Password	(Required) The passphrase for the client private key.	-
CA Certificate to Trust	(Required) The trusted Certificate Authority's (CA) digital certificate.	-



Plaintext Authentication

Caution: Tenable does not recommend plaintext credentials. Instead, use encrypted authentication methods when possible.

If a secure method of performing credentialed checks is not available, you can configure Tenable.sc to perform checks over unsecure protocols using plaintext authentication settings.

Tenable.sc supports the following plaintext authentication methods:

- [telnet/rsh/rexec](#)
- [NNTP](#)
- [FTP](#)
- [POP2](#)
- [POP3](#)
- [IMAP](#)
- [IPMI](#)
- [HTTP](#)

You can configure plaintext authentication options in scan policies, as described in [Authentication Options](#) and [Add a Scan Policy](#).

telnet/rsh/rexec

Tenable.sc performs patch auditing on non-Windows targets only.

Setting	Description	Default
Username	(Required) The username for the telnet, rsh, or rexec account that Tenable.sc uses to perform checks on the target system.	–
Password (Unsafe!)	(Required) The password for the telnet, rsh, or rexec user.	–

NNTP



Setting	Description	Default
Username	(Required) The username for the NNTP account that Tenable.sc uses to perform checks on the target system.	-
Password	(Required) The password for the NNTP user.	-

FTP

Setting	Description	Default
Username	(Required) The username for the FTP account that Tenable.sc uses to perform checks on the target system.	-
Password	(Required) The password for the FTP user.	-

POP2

Setting	Description	Default
Username	(Required) The username for the POP2 account that Tenable.sc uses to perform checks on the target system.	-
Password	(Required) The password for the POP2 user.	-

POP3

Setting	Description	Default
Username	(Required) The username for the POP3 account that Tenable.sc uses to perform checks on the target system.	-
Password	(Required) The password for the POP3 user.	-

IMAP

Setting	Description	Default



Username	(Required) The username for the IMAP account that Tenable.sc uses to perform checks on the target system.	-
Password	(Required) The password for the IMAP user.	-

IPMI

Setting	Description	Default
Username	(Required) The username for the IPMI account that Tenable.sc uses to perform checks on the target system.	-
Password (Sent in Clear)	(Required) The password for the IPMI user.	-

HTTP

Setting	Description	Default
Authentication Method	(Required) The authentication method. • Automatic authentication • Basic/Digest authentication • HTTP login form – Controls the start location of authenticated testing of a custom web-based application. • HTTP cookies import – Tenable.sc uses cookies imported from another piece of software (such as a web browser or web proxy) to facilitate web application testing by using when attempting to access a web application.	HTTP Login Form
Username	(Required) The username for the HTTP account that Tenable.sc uses to perform checks on the target system.	-



Setting	Description	Default
Password	(Required) The password for the HTTP user.	–
Login page	(Required) The absolute path to the application login page. For example, <code>/login.html</code> .	–
Login submission page	(Required) The action parameter for the form method. For example, for <code><form method="POST" name="auth_form" action="/login.php"></code> , use <code>/login.php</code> .	–
Login parameters	(Required) The authentication parameters (for example, <code>login=%USER%&password=%PASS%</code>). Tenable.sc replaces the <code>%USER%</code> and <code>%PASS%</code> keywords with values supplied on the Login configurations drop-down menu. Tip: If needed, you can provide additional parameters, such as a group name or other information required for authentication.	–
Check authentication on page	(Required) The absolute path of a protected web page that requires authentication. For example, <code>/admin.html</code> .	–
Regex to verify successful authentication	(Required) The regex pattern you want Tenable.sc to look for on the login page to validate authentication. Tip: Tenable.sc can attempt to match a given string, such as <code>Authentication successful</code>.	–
Cookies file	(Required) A cookie file in Netscape <code>cookies.txt</code> format.	–



Patch Management

Tenable.sc can leverage credentials for patch management systems to perform patch auditing on systems for which credentials may not be available to the Nessus scanner. Tenable.sc supports:

- [Dell KACE K1000](#)
- [IBM BigFix](#)
- [Microsoft System Center Configuration Manager \(SCCM\)](#)
- [Microsoft Windows Server Update Services \(WSUS\)](#)
- [Red Hat Satellite Server](#)
- [Symantec Altiris](#)

You can configure patch management options in scan policies, as described in [Authentication Options](#) and [Add a Scan Policy](#).

IT administrators are expected to manage the patch monitoring software and install any agents required by the patch management system on their systems.

Note: If the credential check sees a system but it is unable to authenticate against the system, it uses the data obtained from the patch management system to perform the check. If Tenable.sc is able to connect to the target system, it performs checks on that system and ignores the patch management system output.

Note: The data returned to Tenable.sc by the patch management system is only as current as the most recent data that the patch management system has obtained from its managed hosts.

Scanning with Multiple Patch Managers

If you provide multiple sets of credentials to Tenable.sc for patch management tools, Tenable.sc uses all of them.

If you provide credentials for a host and for one or more patch management systems, Tenable.sc compares the findings between all methods and report on conflicts or provide a satisfied finding. Use the Patch Management Windows Auditing Conflicts plugins to highlight patch data differences between the host and a patch management system.

Dell KACE K1000



KACE K1000 is available from Dell to manage the distribution of updates and hotfixes for Linux, Windows, and Mac OS X systems. Tenable.sc can query KACE K1000 to verify whether or not patches are installed on systems managed by KACE K1000 and display the patch information through the Tenable.sc user interface.

Tenable.sc supports KACE K1000 versions 6.x and earlier.

KACE K1000 scanning uses the following Tenable plugins: 76867, 76868, 76866, and 76869.

Option	Description	Default
Server	(Required) The KACE K1000 IP address or system name.	-
Database Port	(Required) The TCP port that KACE K1000 listens on for communications from Tenable.sc.	3306
Organization Database Name	(Required) The name of the organization component for the KACE K1000 database (e.g., ORG1).	ORG1
Database Username	(Required) The username for the KACE K1000 account that Tenable.sc uses to perform checks on the target system.	R1
K1000 Database Password	(Required) The password for the KACE K1000 user.	-

IBM BigFix

IBM BigFix is available to manage the distribution of updates and hotfixes for desktop systems. Tenable.sc can query IBM BigFix to verify whether or not patches are installed on systems managed by IBM BigFix and display the patch information.

Package reporting is supported by RPM-based and Debian-based distributions that IBM BigFix officially supports. This includes Red Hat derivatives such as RHEL, CentOS, Scientific Linux, and Oracle Linux, as well as Debian and Ubuntu. Other distributions may also work, but unless IBM BigFix officially supports them, there is no support available.

For local check plugins to trigger, only RHEL, CentOS, Scientific Linux, Oracle Linux, Debian, Ubuntu, and Solaris are supported. Plugin 65703 must be enabled.

Tenable.sc supports IBM BigFix 9.5 and later and 10.x and later.

IBM BigFix scanning uses the following Tenable plugins: 62558, 62559, 62561, 62560, and 65703.



Option	Description	Default
Web Reports Server	(Required) The name of IBM BigFix Web Reports server.	-
Web Reports Port	(Required) The TCP port that the IBM BigFix Web Reports server listens on for communications from Tenable.sc.	-
Web Reports Username	(Required) The username for the IBM BigFix Web Reports administrator account that Tenable.sc uses to perform checks on the target system.	-
Web Reports Password	(Required) The password for the IBM BigFix Web Reports administrator user.	-
HTTPS	When enabled, Tenable.sc connects using secure communication (HTTPS). When disabled, Tenable.sc connects using standard HTTP.	Enabled
Verify SSL certificate	When enabled, Tenable.sc verifies that the SSL certificate on the server is signed by a trusted CA. Tip: If you are using a self-signed certificate, disable this setting.	Enabled

IBM BigFix Server Configuration

In order to use these auditing features, you must make changes to the IBM BigFix server. You must import a custom analysis into IBM BigFix so that detailed package information is retrieved and made available to Tenable.sc.

From the HCL BigFix Console application, import the following .bes files.

BES file:

```
<?xml version="1.0" encoding="UTF-8"?>
<BES xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="BES.xsd">
  <Analysis>
    <Title>Tenable</Title>
    <Description>This analysis provides SecurityCenter with the data it needs for vulnerability reporting. <
    <Relevance>true</Relevance>
    <Source>Internal</Source>
```



```
<SourceReleaseDate>2013-01-31</SourceReleaseDate>
<MIMEField>
  <Name>x-fixlet-modification-time</Name>
  <Value>Thu, 13 May 2021 21:43:29 +0000</Value>
</MIMEField>
<Domain>BES</Domain>
<Property Name="Packages - With Versions (Tenable)" ID="74">if (exists true whose (if true then
repository) else false)) then unique values of (lpp_name of it &amp; "|" &amp; version of it as string &amp; "|" &amp; "fileset"
tecture of operating system) of filesets of products of object repository else if (exists true whose (if true then
anpackage) else false)) then unique values of (name of it &amp; "|" &amp; version of it as string &amp; "|" &amp; "deb" &amp; "|" &amp;
it &amp; "|" &amp; architecture of operating system) of packages whose (exists version of it) of debianpackages else if
whose (if true then (exists rpm) else false)) then unique values of (name of it &amp; "|" &amp; version of it as string
"&amp;|" &amp; architecture of it &amp; "|" &amp; architecture of operating system) of packages of rpm else if (exists true whose
(exists ips image) else false)) then unique values of (full name of it &amp; "|" &amp; version of it as string &amp; "|" &amp;
architecture of operating system) of latest installed packages of ips image else if (exists true whose (if true
pkgdb) else false)) then unique values of (pkginst of it &amp; "|" &amp; version of it &amp; "|" &amp; "pkg10") of pkginfos of pk
"&lt;unsupported&gt;"]]&gt;&lt;/Property&gt;
  &lt;Property Name="Tenable AIX Technology Level" ID="76"&gt;current technology level of operating system&lt;/Property&gt;
  &lt;Property Name="Tenable Solaris - Showrev -a" ID="77"&gt;<![CDATA[if ((operating system as string as lowercase
"SunOS 5.10" as lowercase) AND (exists file "/var/opt/BESClient/showrev_patches.b64")) then lines of file "/var/
opt/BESClient/showrev_patches.b64" else "&lt;unsupported&gt;"]]&gt;&lt;/Property&gt;
&lt;/Analysis&gt;
&lt;/BES&gt;</pre></div><div data-bbox="65 427 150 444" data-label="Section-Header"><h2>BES File:</h2></div><div data-bbox="90 476 913 873" data-label="Text"><pre>&lt;?xml version="1.0" encoding="UTF-8"?&gt;
&lt;BES xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="BES.xsd"&gt;
  &lt;Task&gt;
    &lt;Title&gt;Tenable - Solaris 5.10 - showrev -a Capture&lt;/Title&gt;
    &lt;Description&gt;&lt;![CDATA[&amp;lt;enter a description of the task here&amp;gt; ]]&gt;&lt;/Description&gt;
    &lt;GroupRelevance JoinByIntersection="false"&gt;
      &lt;SearchComponentPropertyReference PropertyName="OS" Comparison="Contains"&gt;
        &lt;SearchText&gt;SunOS 5.10&lt;/SearchText&gt;
        &lt;Relevance&gt;exists (operating system) whose (it as string as lowercase contains "SunOS
5.10" as lowercase)&lt;/Relevance&gt;
      &lt;/SearchComponentPropertyReference&gt;
    &lt;/GroupRelevance&gt;
    &lt;Category&gt;&lt;/Category&gt;
    &lt;Source&gt;Internal&lt;/Source&gt;
    &lt;SourceID&gt;&lt;/SourceID&gt;
    &lt;SourceReleaseDate&gt;2021-05-12&lt;/SourceReleaseDate&gt;
    &lt;SourceSeverity&gt;&lt;/SourceSeverity&gt;
    &lt;CVENames&gt;&lt;/CVENames&gt;
    &lt;SANSID&gt;&lt;/SANSID&gt;
    &lt;MIMEField&gt;
      &lt;Name&gt;x-fixlet-modification-time&lt;/Name&gt;
      &lt;Value&gt;Thu, 13 May 2021 21:50:58 +0000&lt;/Value&gt;
    &lt;/MIMEField&gt;
    &lt;Domain&gt;BES&lt;/Domain&gt;
    &lt;DefaultAction ID="Action1"&gt;
      &lt;Description&gt;
        &lt;PreLink&gt;Click &lt;/PreLink&gt;
        &lt;Link&gt;here&lt;/Link&gt;
        &lt;PostLink&gt; to deploy this action.&lt;/PostLink&gt;
      &lt;/Description&gt;</pre></div><div data-bbox="54 938 936 963" data-label="Page-Footer"><p>Copyright © 2021 Tenable, Inc. All rights reserved. Tenable, Tenable.io, Tenable Network Security, Nessus, SecurityCenter, SecurityCenter Continuous View and Log Correlation Engine are registered trademarks of Tenable, Inc. Tenable.sc, Tenable.ot, Lumin, Indegy, Assure, and The Cyber Exposure Company are trademarks of Tenable, Inc. All other products or services are trademarks of their respective</p></div>
```



```
<ActionScript MIMEType="application/x-sh"><![CDATA[#!/bin/sh
/usr/bin/showrev -a > /var/opt/BESClient/showrev_patches
/usr/sfw/bin/openssl base64 -in /var/opt/BESClient/showrev_patches -out /var/opt/BESClient/showrev_
patches.b64

]]></ActionScript>
</DefaultAction>
</Task>
</BES>
```

Microsoft System Center Configuration Manager (SCCM)

Microsoft System Center Configuration Manager (SCCM) is available to manage large groups of Windows-based systems. Tenable.sc can query the SCCM service to verify whether or not patches are installed on systems managed by SCCM and display the patch information through the scan results.

Tenable.sc connects to the server that is running the SCCM site (e.g., credentials must be valid for the SCCM service, so the selected user must have privileges to query all the data in the SCCM MMC). This server may also run the SQL database, or the database and the SCCM repository can be on separate servers. When leveraging this audit, Tenable.sc must connect to the SCCM server via WMI and HTTPS.

SCCM scanning uses the following Tenable plugins: 57029, 57030, 73636, and 58186.

Note: SCCM patch management plugins support SCCM 2007, SCCM 2012, SCCM 2016, and SCCM 2019.

Credential	Description	Default
Server	(Required) The SCCM IP address or system name.	-
Domain	(Required) The name of the SCCM server's domain.	-
Username	(Required) The username for the SCCM user account that Tenable.sc uses to perform checks on the target system. The user account must have privileges to query all data in the SCCM MMC.	-
Password	(Required) The password for the SCCM user with privileges to query all data in the SCCM MMC.	-

Windows Server Update Services (WSUS)



Windows Server Update Services (WSUS) is available from Microsoft to manage the distribution of updates and hotfixes for Microsoft products. Tenable.sc can query WSUS to verify whether or not patches are installed on systems managed by WSUS and display the patch information through the Tenable.sc user interface.

WSUS scanning uses the following Tenable plugins: 57031, 57032, and 58133.

Option	Description	Default
Server	(Required) The WSUS IP address or system name.	-
Port	(Required) The TCP port that Microsoft WSUS listens on for communications from Tenable.sc.	8530
Username	(Required) The username for the WSUS administrator account that Tenable.sc uses to perform checks on the target system.	-
Password	(Required) The password for the WSUS administrator user.	-
HTTPS	When enabled, Tenable.sc connects using secure communication (HTTPS). When disabled, Tenable.sc connects using standard HTTP.	Enabled
Verify SSL Certificate	When enabled, Tenable.sc verifies that the SSL certificate on the server is signed by a trusted CA. Tip: If you are using a self-signed certificate, disable this setting.	Enabled

Red Hat Satellite Server

Red Hat Satellite is a systems management platform for Linux-based systems. Tenable.sc can query Satellite to verify whether or not patches are installed on systems managed by Satellite and display the patch information.



Although not supported by Tenable, the Red Hat Satellite plugin also works with Spacewalk Server, the Open Source Upstream Version of Red Hat Satellite. Spacewalk can manage distributions based on Red Hat (RHEL, CentOS, Fedora) and SUSE. Tenable supports the Satellite server for Red Hat Enterprise Linux.

Satellite scanning uses the following Tenable plugins: 84236, 84235, 84234, 84237, and 84238.

Option	Description	Default
Satellite Server	(Required) The Red Hat Satellite IP address or system name.	-
Port	(Required) The TCP port that Red Hat Satellite listens on for communications from Tenable.sc.	443
Username	(Required) The username for the Red Hat Satellite account that Tenable.sc uses to perform checks on the target system.	-
Password	(Required) The password for the Red Hat Satellite user.	-
Verify SSL Certificate	When enabled, Tenable.sc verifies that the SSL certificate on the server is signed by a trusted CA. Tip: If you are using a self-signed certificate, disable this setting.	Enabled

Red Hat Satellite 6 Server

Red Hat Satellite 6 is a systems management platform for Linux-based systems. Tenable.sc can query Satellite to verify whether or not patches are installed on systems managed by Satellite and display the patch information.

Although not supported by Tenable, the Red Hat Satellite 6 plugin also works with Spacewalk Server, the Open Source Upstream Version of Red Hat Satellite. Spacewalk can manage distributions based on Red Hat (RHEL, CentOS, Fedora) and SUSE. Tenable supports the Satellite server for Red Hat Enterprise Linux.

Red Hat Satellite 6 scanning uses the following Tenable plugins: 84236, 84235, 84234, 84237, 84238, 84231, 84232, and 84233.



Option	Description	Default
Satellite Server	(Required) The Red Hat Satellite 6 IP address or system name.	-
Port	(Required) The TCP port that Red Hat Satellite 6 listens on for communications from Tenable.sc.	443
Username	(Required) The username for the Red Hat Satellite 6 account that Tenable.sc uses to perform checks on the target system.	-
Password	(Required) The password for the Red Hat Satellite 6 user.	-
HTTPS	When enabled, Tenable.sc connects using secure communication (HTTPS). When disabled, Tenable.sc connects using standard HTTP.	Enabled
Verify SSL Certificate	When enabled, Tenable.sc verifies that the SSL certificate on the server is signed by a trusted CA. Tip: If you are using a self-signed certificate, disable this setting.	Enabled

Symantec Altiris

Altiris is available from Symantec to manage the distribution of updates and hotfixes for Linux, Windows, and Mac OS X systems. Tenable.sc has the ability to use the Altiris API to verify whether or not patches are installed on systems managed by Altiris and display the patch information through the Tenable.sc user interface.

Tenable.sc connects to the Microsoft SQL server that is running on the Altiris host. When leveraging this audit, if the MSSQL database and Altiris server are on separate hosts, Tenable.sc must connect to the MSSQL database, not the Altiris server.

Altiris scanning uses the following Tenable plugins: 78013, 78012, 78011, and 78014.



Credential	Description	Default
Server	(Required) The Altiris IP address or system name.	-
Database Port	(Required) The TCP port that Altiris listens on for communications from Tenable.sc.	5690
Database Name	(Required) The name of the MSSQL database that manages Altiris patch information.	Symantec_CMDB
Database Username	(Required) The username for the Altiris MSSQL database account that Tenable.sc uses to perform checks on the target system. Credentials must be valid for a MSSQL database account with the privileges to query all the data in the Altiris MSSQL database.	-
Database Password	(Required) The password for the Altiris MSSQL database user.	-
Use Windows Authentication	When enabled, use NTLMSSP for compatibility with older Windows Servers. When disabled, use Kerberos.	Enabled



View Your Scan Policies

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

For more information, see [Scan Policies](#).

To view a list of configured scan policies:

1. Log in to Tenable.sc via the user interface.
2. Click **Scanning > Policies** (administrator users) or **Scans > Policies** (organizational users).

The **Policies** page appears.

3. View details about each scan policy.
 - **Name** — The name of the scan policy.
 - **Tag** — The tag applied to the scan policy.
 - **Type** — The name of the template used to add the scan policy.
 - **Group** — The group associated with the scan policy.
 - **Owner** — The username for the user associated with the scan policy.
 - **Last Modified** — The date and time the scan policy was last modified.



View Scan Policy Details

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

You can view details for individual scan policies. For more information, see [Scan Policies](#).

To view details of a scan policy:

1. Log in to Tenable.sc via the user interface.
2. Click **Scanning > Policies** (administrator users) or **Scans > Policies** (organizational users).

The **Policies** page appears.

3. In the row for the scan policy you want to view, click the  menu.

The actions menu appears.

4. Click **View**.

The **View Policy** page appears.

Section	Action
General	View general information for the scan policy. • Name – The name of the scan policy. • Description – The description for the scan policy. • Tag – The tag applied to the scan policy. • Type – The name of the template used to add the scan policy. • Created – The date and time the scan policy was added. • Last Modified – The date and time the scan policy was last modified. • Owner – The username for the user associated with the scan policy.



Section	Action
	• Group – The group associated with the scan policy. • ID – The scan policy ID.
Configuration	(Template-based policies only) View a summary of options configured for the scan policy. For more information, see Scan Policy Options .
Options tabs	View all of the options configured for the scan policy. The tabs displayed depend on the scan policy type. For more information, see Scan Policy Options .



Edit a Scan Policy

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

For more information, see [Scan Policies](#).

To edit a scan policy:

1. Log in to Tenable.sc via the user interface.
2. Click **Scanning > Policies** (administrator users) or **Scans > Policies** (organizational users).

The **Policies** page appears.

3. In the row for the scan policy you want to edit, click the  menu.

The actions menu appears.

4. Click **Edit**.

The **Edit Policy** page appears.

5. Modify the scan policy. For more information, see [Scan Policy Options](#).
6. Click **Submit**.

Tenable.sc saves your configuration.



Share or Revoke Access to a Scan Policy

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

You can share or revoke access to a scan policy to allow or restrict access to a user group. When you share a scan policy with a user group, users in the group with the appropriate permissions can use the policy in an active scan, modify policy options, and more.

For more information, see [Scan Policies](#). For more information about user groups, see [Groups](#).

To share or revoke access to a scan policy:

1. Log in to Tenable.sc via the user interface.
2. Click **Scanning > Policies** (administrator users) or **Scans > Policies** (organizational users).

The **Policies** page appears.

3. In the row for the scan policy for which you want to share or revoke access, click the  menu.

The actions menu appears.

4. Click **Share**.

The **Share Policy** window appears.

5. In the **Share Policy** window, select the groups for which you want to share or revoke access to the scan policy.
6. Click **Submit**.

Tenable.sc saves your configuration.



Export a Scan Policy

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

You can export a scan policy as a .nessus file and import it to another Tenable.sc to use in an active scan configuration.

In some cases, Tenable Support may also ask you to export a scan policy for troubleshooting.

Note: Exported scan policy files do not include audit files or credentials. You can re-configure audit files and credentials you want to use with the scan policy on the Tenable.sc where you import the scan policy. For more information, see [Audit Files](#) and [Credentials](#).

For more information, see [Scan Policies](#).

Before you begin:

- Add a scan policy, as described in [Add a Scan Policy](#).
- Confirm your **PHP Serialization Mode** setting is set to **PHP Serialization ON**. For more information, see [Security Settings](#).

To export a scan policy:

1. Log in to Tenable.sc via the user interface.
2. Click **Scanning > Policies** (administrator users) or **Scans > Policies** (organizational users).

The **Policies** page appears.

3. In the row for the scan policy you want to export, click the  menu.

The actions menu appears.

4. Click **Export**.

Tenable.sc exports the scan policy as a .xml file.

What to do next:



- Do any of the following:
 - Import the scan policy into another Tenable.sc, as described in [Import a Scan Policy](#).
 - If Tenable Support requested a scan policy file for troubleshooting, share the scan policy file with Tenable Support.



Import a Scan Policy

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

You can import a .nessus scan policy file from Nessus or from another Tenable.sc to use in an active scan configuration. For more information, see [Scan Policies](#).

Note: Imported scan policies do not include audit files or credentials. For more information, see [Audit Files](#) and [Credentials](#).

Before you begin:

- Ensure your **PHP Serialization Mode** setting is **PHP Serialization ON**. For more information, see [Security Settings](#).
- Do one of the following:
 - Export a scan policy from another Tenable.sc, as described in [Export a Scan Policy](#).
 - Export a scan policy from Nessus. For more information, see [Policies](#) in the *Nessus User Guide*.

To import a scan policy:

1. Log in to Tenable.sc via the user interface.
2. Click **Scanning > Policies** (administrator users) or **Scans > Policies** (organizational users).

The **Policies** page appears.

3. In the top right corner of the page, click **Options**.

The options menu appears.

4. Click **Upload Policy**.

The **Upload Policy** page appears.

5. In the **Name** box, type a name for the scan policy.
6. (Optional) In the **Description** box, type a description for the scan policy.



7. (Optional) In the **Tag** box, type or select a tag for the scan policy.
8. Click **Choose File** and browse to the .nessus scan policy file you want to import.
9. Click **Submit**.

Tenable.sc imports the scan policy.

What to do next:

- (Optional) Modify the scan policy settings, as described in [Edit a Scan Policy](#).
- (Optional) Configure audit files and credentials you wish to reference with the scan policy, as described in [Add a Custom Audit File](#) and [Add Credentials](#).
- Reference the scan policy in an active scan configuration, as described in [Add an Active Scan](#).



Copy a Scan Policy

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

For more information, see [Scan Policies](#).

To create a copy of a scan policy:

1. Log in to Tenable.sc via the user interface.
2. Click **Scanning > Policies** (administrator users) or **Scans > Policies** (organizational users).

The **Policies** page appears.

3. In the row for the scan policy you want to copy, click the  menu.

The actions menu appears.

4. Click **Copy**.

Tenable.sc copies the scan policy. The copy appears, named **Copy of PolicyName**.



Delete a Scan Policy

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

For more information, see [Scan Policies](#).

Note: If you delete a scan policy referenced by an active scan, Tenable.sc disables the scan. For more information, see [Scan Result Statuses](#).

Before you begin:

- If any active scans reference the scan policy you intend to delete, update the active scans to use a different scan policy, as described in [Manage Active Scans](#).

To delete a scan policy:

1. Log in to Tenable.sc via the user interface.
2. Click **Scanning > Policies** (administrator users) or **Scans > Policies** (organizational users).

The **Policies** page appears.

3. In the row for the scan policy you want to delete, click the  menu.

The actions menu appears.

4. Click **Delete**.

A confirmation window appears.

5. Click **Delete**.

Tenable.sc deletes the scan policy.



Agent Scanning

To perform agent scanning, Tenable.sc fetches agent scan results from agent-capable Nessus Manager or Tenable.io instances. Using Nessus Agents for scanning reduces network usage and allows devices to maintain their scan schedules even when disconnected from the network. Tenable.sc fetches these results for review in conjunction with other acquired information about the host and network.

You can configure one or both methods of fetching agent scan results in Tenable.sc:

- *Agent scans* fetch results from agent scans you add and launch in Tenable.sc. When you add an agent scan in Tenable.sc, Tenable.sc creates a corresponding agent scan in an instance of Nessus Manager or Tenable.io that you linked to Tenable.sc. When you launch an agent scan in Tenable.sc, Tenable.sc launches the corresponding scan in Nessus Manager or Tenable.io, then imports the results into Tenable.sc.

You can create agent scans in Tenable.sc using only the Basic Agent Scan template the Basic Agent Scan template or the Advanced Agent Scan template. For more information, see [Agent Scan and Policy Templates](#) in the *Nessus Agent Deployment and User Guide* and [Tenable-Provided Agent Templates](#) in the *Tenable.io User Guide*. For more information, see [Scan Policy Templates](#).

For more information, see [Agent Scans](#).

- *Agent synchronization jobs* fetch results from agent scans you previously created and launched in Nessus Manager or Tenable.io.

Agent synchronization jobs can fetch results from agent scans configured in Nessus Manager or Tenable.io using any agent scan template.

For more information, see [Agent Synchronization Jobs](#).

To configure agent scanning:

1. Configure Nessus Agents in either Nessus Manager or Tenable.io, as described in [Deployment Workflow](#) in the *Nessus Agent Deployment and User Guide*.
2. Add your agent-capable Nessus Manager or Tenable.io instance as a Nessus scanner in Tenable.sc, as described in [Nessus Scanners](#).



3. Add one or more agent repositories in Tenable.sc, as described in [Add a Repository](#).
4. Do one or both of the following:
 - Add an agent scan using the Basic Agent Scan or Advanced Agent Scan template in Tenable.sc, as described in [Add an Agent Scan](#).
 - Add an agent synchronization job in Tenable.sc, as described in [Add an Agent Synchronization Job](#).

What to do next:

- View scan results, as described in [Scan Results](#).
- View vulnerability data by unique Agent ID, as described in [Vulnerability Analysis](#).



Agent Scans

Agent scans fetch results from agent scans you add and launch in Tenable.sc. When you add an agent scan in Tenable.sc, Tenable.sc creates a corresponding agent scan in an instance of Nessus Manager or Tenable.io that you linked to Tenable.sc. When you launch an agent scan in Tenable.sc, Tenable.sc launches the corresponding scan in Nessus Manager or Tenable.io, then imports the results into Tenable.sc.

You can create agent scans in Tenable.sc using only the Basic Agent Scan template the Basic Agent Scan template or the Advanced Agent Scan template. For more information, see [Agent Scan and Policy Templates](#) in the *Nessus Agent Deployment and User Guide* and [Tenable-Provided Agent Templates](#) in the *Tenable.io User Guide*. For more information, see [Scan Policy Templates](#).

For more information about agent scanning in Tenable.sc, see [Agent Scanning](#).

The **Agent Scans** page displays a list of all available agent scans. Newly created agent scan import schedules are shared to everyone within the same user group when users have the appropriate permissions.

When more than one agent scan result is ready on Tenable.io or Nessus Manager, the scan results queue for import to Tenable.sc.

For more information about agent scans, see:

- [Add an Agent Scan](#)
- [Agent Scan Settings](#)
- [Manage Agent Scans](#)



Add an Agent Scan

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

You can create agent scans in Tenable.sc using only the Basic Agent Scan template, the Basic Agent Scan template or the Advanced Agent Scan template. For more information, see [Agent Scan and Policy Templates](#) in the *Nessus Agent Deployment and User Guide* and [Tenable-Provided Agent Templates](#) in the *Tenable.io User Guide*. For more information, see [Scan Policy Templates](#).

For more information, see [Agent Scans](#) and [Agent Scan Settings](#).

Before you begin:

- Confirm you understand the complete agent scanning configuration process, as described in [Agent Scanning](#).
- (Optional) Configure an Advanced Agent Scan policy template, as described in [Add a Scan Policy](#).

To add an agent scan:

1. Log in to Tenable.sc via the user interface.
2. Click **Scans > Agent Scans**.

The **Agent Scans** page appears.

3. Click **Add**.

The **Add Agent Scan** page appears.

4. Click **General**.
5. Type a **Name** for the scan.
6. (Optional) Type a **Description** for the scan.
7. (Optional) To reference an Advanced Agent Scan policy in the scan:
 - a. Click **Custom Policy** to enable the toggle.
 - b. In the **Policy** drop-down menu, select the Advanced Agent Scan policy.



8. Select an **Agent Scanner**.
9. Select one or more **Agent Groups**.
10. Select a **Scan Window**.
11. (Optional) Select a **Schedule** for the scan.
12. Click **Settings**.
13. Select an **Import Repository** for the scan.
14. (Optional) Click **Post Scan**.
 - If you want to configure automatic report generation, click **Add Report**. For more information, see [Add a Report to a Scan](#).
15. Click **Submit**.

Tenable.sc saves your configuration.

What to do next:

- View scan results, as described in [Scan Results](#).
- View vulnerability data by unique Agent ID, as described in [Vulnerability Analysis](#).



Manage Agent Scans

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

For more information about agent scans, see [Agent Scans](#).

To manage agent scans:

1. Log in to Tenable.sc via the user interface.
2. Click **Scans > Agent Scans**.

The **Agent Scans** page appears.

3. To filter the scans that appear on the page, apply a filter as described in [Apply a Filter](#).
4. To start or pause a scan, see [Start or Pause a Scan](#).
5. To view details for a scan:

- a. In the row for the scan, click the  menu.

The actions menu appears.

- b. Click **View**.

The **View Agent Scan** page appears.

6. To edit a scan:

- a. In the row for the scan, click the  menu.

The actions menu appears.

- b. Click **Edit**.

The **Edit Agent Scan** page appears.

- c. Modify the scan options. For more information, see [Agent Scan Settings](#).
- d. Click **Submit**.

Tenable.sc saves your configuration.



7. To delete a scan:

- a. In the row for the scan, click the  menu.

The actions menu appears.

- b. Click **Delete**.

Tenable.sc deletes the scan.



Start or Pause a Scan

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

To start or pause an active scan, agent scan, or agent synchronization job:

1. Log in to Tenable.sc.
2. Click one of the following:
 - **Scans > Active Scans** (to manage active scans)
 - **Scans > Agent Synchronization Jobs** (to manage agent synchronization jobs)
 - **Scans > Agent Scans** (to manage agent scans)
 - **Scans > Scan Results** (to manage a scan from the results page).
3. Do one of the following:
 - To pause the scan or synchronization job, click the pause button on the right side of the scan or synchronization job row.
 - To start the scan or synchronization job, click the start button on the right side of the scan or synchronization job row.



Agent Scan Settings

For more information, see [Agent Scans](#).

- [General Options](#)
- [Settings Options](#)
- [Post Scan Options](#)

General Options

Parameter	Description	Default
General		
Name	The scan name associated with the scan's results. This may be any name or phrase (e.g., SystemA, DMZ Scan, Daily Scan of the Web Farm , etc.).	--
Description	Descriptive information related to the scan.	--
Custom Policy	When enabled, select an agent scan policy to apply to the scan. For more information, see Scan Policy Templates . When disabled, the scan uses a Nessus or Tenable.io Basic Agent Scan template. For more information, see Agent Scan and Policy Templates in the <i>Nessus Agent Deployment and User Guide</i> and Tenable-Provided Agent Templates in the <i>Tenable.io User Guide</i> .	Disabled
Policy	(If Custom Policy is enabled) The name of the agent scan policy.	--
Agent Scanner	The Agent-enabled scanner from which to retrieve agent results.	--
Agent Groups	Specifies the agent group or groups in Nessus Manager you want the scan to target. For more information, see Agent Groups in the <i>Nessus User Guide</i> .	--



Parameter	Description	Default
Scan Window	Specifies the amount of time Tenable.sc waits before fetching the results of the agent scan: 15 minutes, 30 minutes, 1 hour, 3 hours, 6 hours, 12 hours, or 1 day. If Tenable.sc fetches results for the scan before the scan completes, Tenable.sc displays the results available at the time the scan window expired. The agent scan continues to run in Tenable.io or Nessus Manager for the duration of the scan window specified in Tenable.io or Nessus Manager, even if the scan window in Tenable.sc expires. Note: To view complete agent scan result data in Tenable.sc, Tenable recommends setting a Scan Window value that allows your agent scans to complete before Tenable.sc fetches the results.	1 hour
Schedule		
Schedule	The frequency you want Tenable.sc to fetch agent scan results: Now, Remediation, Once, Daily, Weekly, Monthly, or On Demand. Note: If you schedule your scan to repeat monthly, Tenable recommends setting a start date no later than the 28th day. If you select a start date that does not exist in some months (e.g., the 29th), Tenable.sc cannot run the scan on those days. Tip: You should retrieve agent scan results as close to the completion time of the scan as possible to most accurately display within Tenable.sc when the scan discovered the vulnerability results.	On Demand

Settings Options

Parameter	Description	Default
Import Repository	Specifies the repository where you want the agent scan results to import. Select an agent repository to receive scan	--



Parameter	Description	Default
	data. Note: You cannot import agent scan data to a non-agent repository.	

Post Scan Options

These options determine what actions occurs immediately before and after the agent scan completes.

Option	Description	Default
Add Report	This option provides a list of reports available to the user to run when the agent scan data import completes. For more information, see Add a Report to a Scan .	--



Agent Synchronization Jobs

Agent synchronization jobs fetch results from agent scans you previously created and launched in Nessus Manager or Tenable.io. Agent synchronization jobs can fetch results from agent scans configured in Nessus Manager or Tenable.io using any agent scan template. For more information about agent scanning in Tenable.sc, see [Agent Scanning](#).

The **Agent Synchronization Jobs** page displays a list of all available agent synchronization jobs. Newly created agent scan import schedules are shared to everyone within the same user group when users have the appropriate permissions.

When more than one agent scan result is ready on Nessus Manager, the scan results queue for import to Tenable.sc.

For more information about agent synchronization jobs, see:

- [Add an Agent Synchronization Job](#)
- [Agent Synchronization Job Settings](#)
- [Manage Agent Synchronization Jobs](#)



Add an Agent Synchronization Job

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

For more information about agent synchronization jobs, see [Agent Synchronization Jobs](#). For more information about agent synchronization job options, see [Agent Synchronization Job Settings](#).

Before you begin:

- Confirm you understand the complete agent scanning configuration process, as described in [Agent Scanning](#).

To add an agent synchronization job:

1. Log in to Tenable.sc via the user interface.
2. Click **Scans > Agent Synchronization Jobs**.

The **Agent Synchronization Jobs** page appears.

3. Click **Add**.

The **Add Agent Synchronization Job** page appears.

4. Click **General**.
5. Type a **Name** for the agent synchronization job.
6. (Optional) Type a **Description** for the agent synchronization job.
7. Select an **Agent Scanner**.
8. Type an **Agent Scan Name Filter**.
9. (Optional) If you want to limit the scan results fetched by Tenable.sc, enable **Scan Result Threshold** and select a date and time to specify the oldest scan results you want Tenable.sc to fetch.
10. (Optional) Select a **Schedule** for the agent synchronization job.
11. Click **Settings**.
12. Select an **Import Repository** for the agent synchronization job.



13. (Optional) Click **Post Scan**.

- If you want to configure automatic report generation, click **Add Report**. For more information, see [Add a Report to a Scan](#).
- If you previously added an email address to your account profile and you want to configure email notifications, enable or disable **E-Mail Me on Launch** or **E-Mail Me on Completion**.

14. Click **Submit**.

Tenable.sc saves your configuration.

What to do next:

- View scan results, as described in [Scan Results](#).
- View vulnerability data by unique Agent ID, as described in [Vulnerability Analysis](#).



Manage Agent Synchronization Jobs

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

For more information, see [Agent Synchronization Jobs](#).

To manage agent synchronization jobs:

1. Log in to Tenable.sc via the user interface.
2. Click **Scans > Agent Synchronization Jobs**.

The **Agent Synchronization Jobs** page appears.

3. To filter the agent synchronization jobs that appear on the page, apply a filter as described in [Apply a Filter](#).
4. To start or pause an agent synchronization job, see [Start or Pause a Scan](#).
5. To view details for an agent synchronization job:
 - a. In the row for the agent synchronization job, click the  menu.

The actions menu appears.

- b. Click **View**.

The **View Agent Synchronization Job** page appears.

6. To edit an agent synchronization job:
 - a. In the row for the agent synchronization job, click the  menu.

The actions menu appears.

- b. Click **Edit**.

The **Edit Agent Synchronization Job** page appears.

- c. Modify the agent synchronization job options. For more information, see [Agent Synchronization Job Settings](#).
- d. Click **Submit**.



Tenable.sc saves your configuration.

7. To copy an agent synchronization job:

- a. In the row for the agent synchronization job, click the  menu.

The actions menu appears.

- b. Click **Copy**.

Tenable.sc creates a copy of the agent synchronization job.

8. To delete an agent synchronization job:

- a. In the row for the agent synchronization job, click the  menu.

The actions menu appears.

- b. Click **Delete**.

Tenable.sc deletes the agent synchronization job.



Agent Synchronization Job Settings

For more information, see [Agent Synchronization Jobs](#).

- [General Options](#)
- [Settings Options](#)
- [Post Scan Options](#)

General Options

Option	Description
Name	The agent synchronization job name associated with the scan's results. This may be any name or phrase (e.g., SystemA , DMZ Scan , Daily Scan of the Web Farm , etc.).
Description	A description for the agent synchronization job.
Agent Scanner	The agent-capable scanner from which you want Tenable.sc to retrieve agent results.
Agent Scan Name Filter	A filter for agent scan results to retrieve from the Nessus Agent-enabled scanner. Filters can use the specific name of the result(s) to retrieve or an asterisk (*) or question mark (?) for all or part of the scan result name(s) to retrieve. You can find the available agent scans retrieved from the selected scanner on the Scan page of the user logged in to the Nessus server. You can click the Preview Filter button to view results that match the filter.
Scan Result Threshold	Specifies whether Tenable.sc fetches all or some agent scan results from the agent-capable scanner. • When disabled, Tenable.sc fetches all agent scan results. • When enabled, Tenable.sc restricts the agent scan results it fetches. Note: You cannot modify the Scan Result Threshold after initial creation of the agent synchronization job.



Option	Description
	After you create the agent synchronization job, the Edit Agent Synchronization Job and View Agent Synchronization Job pages display the Last Fetched date to indicate when Tenable.sc performed the most recent successful agent synchronization job.
Select Date and Time	When Scan Result Threshold is enabled, specifies the oldest agent scan results you want Tenable.sc to fetch.
Schedule	The frequency you want Tenable.sc to fetch agent scan results. Select Now, Once, Daily, Weekly, Monthly, On Demand, or Dependent to create an agent scan result retrieval template that you can launch manually at any time. The other time frames allow you to retrieve agent scan results at specified times and intervals. Tenable recommends retrieving agent scan results as close to the completion time of the scan as possible to most accurately display within Tenable.sc when the scan discovered the vulnerability results. For more information about how Tenable.sc determines vulnerability discovery dates, see Vulnerability Discovered. Note: If you schedule your scan to repeat monthly, Tenable recommends setting a start date no later than the 28th day. If you select a start date that does not exist in some months (e.g., the 29th), Tenable.sc cannot run the scan on those days.

Settings Options

Parameter	Description
Import Repository	Specifies the agent repository where you want the agent scan results to import. Note: You cannot import agent scan data to a non-agent repository.

Post Scan Options



These options determine what actions occurs immediately before and after the agent synchronization job completes. The table below describes the post agent synchronization job options available to users:

Option	Description
Add Report	This option provides a list of reports available to the user to run when the agent scan data import completes. The initial choices are to click the group and owner of the report to present a list of valid report options. Next, click the report from the list that can be searched using the text search box. When hovering over a report name, you can select the information icon to display the name and description of the report. You can base the generated report on the current scan's results or the results in the Cumulative database. Selecting the check mark causes the report to launch once the agent synchronization job completes. Selecting the X removes the changes. Once added, you can modify or delete the report information.



Blackout Windows

You can set a *blackout window* in Tenable.sc to specify a time frame when you do not want Tenable.sc to scan specific targets. This prevents remediation or ad-hoc scans from running during undesired time frames, such as during production hours. For more information about what happens to in-progress scans at the start of a blackout window, see the [knowledge base](#) article.

Blackout windows are organizational and affect all scans in the creating user's organization. Only users with the Manage Blackout Windows permission can add, edit, or delete blackout windows.

For more information, see [Add a Blackout Window](#), [Edit a Blackout Window](#), and [Delete a Blackout Window](#).

Blackout Window Options

Option	Description
Name	A name for the blackout window.
Description	(Optional) A description for the blackout window.
Enabled	When enabled, Tenable.sc does not run scans during the blackout window. When disabled, scans run as scheduled.
Targets	Specifies the targets you do not want to scan during the blackout window. • All Systems – Tenable.sc does not run any scans. • Assets – Tenable.sc does not run any scans on specific Tenable-provided asset types. • IPs – Tenable.sc does not run any scans on specific IP addresses. • Mixed – Tenable.sc does not run any scans on a combination of Tenable-provided asset types or IP addresses. Note: If you select an Import Repository later in the configuration, Tenable.sc applies your Target selections only to scans configured with that import repository. Scans configured with other import repositories still run and scan targeted assets, regardless of your blackout window Targets selection.



Option	Description
Assets	If you selected Assets or Mixed as the Targets , specifies one or more Tenable-provided asset types that you do not want to scan during the blackout window.
IPs	If you selected IPs or Mixed as the Targets , specifies one or more asset IP addresses that you do not want to scan during the blackout window.
ImportRepository	(Optional) If you selected Assets, IPs, or Mixed as your Targets, specifies whether you want to restrict the blackout window to apply to scans configured with a specific import repository. • If you select a repository, Tenable.sc applies the blackout window to scans with the repository configured. • If you do not select a repository, Tenable.sc does not restrict the blackout by repository.
Starts On Frequency Repeat Every Repeat On	Specifies a schedule for the blackout window.



Add a Blackout Window

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

For more information about configuration options, see [Blackout Windows](#).

To add a blackout window:

1. Log in to Tenable.sc via the user interface.
2. Click **Scans > Blackout Windows**.

The **Blackout Windows** page appears.

3. Click **Add**.

The **Add Blackout Window** page appears.

4. In the **Name** box, type a name for the blackout window.
5. In the **Description** box, type a description for the blackout window.
6. Confirm the **Enabled** toggle is enabled.
7. In the **Targets** drop-down box, select a target: **All Systems**, **Assets**, **IPs**, or **Mixed**.

Additional options appear based on the targets you specified.

8. In the **Assets** and/or **IPs** boxes, select or type targets for the blackout window.
9. (Optional) If you selected **Assets** or **Mixed** as the **Targets** and you want to restrict the blackout window by scan repository, in the **Repository** section, select a repository.
10. Modify the **Starts On**, **Frequency**, **Repeat Every**, and **Repeat On** options to set the schedule for the blackout window.
11. Click **Submit**.

Tenable.sc saves your configuration.



Edit a Blackout Window

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

To edit a blackout window:

1. Log in to Tenable.sc via the user interface.
2. Click **Scans > Blackout Windows**.

The **Blackout Windows** page appears.

3. In the row for the blackout window you want to edit, click the  menu.

The actions menu appears.

4. Click **Edit**.

The **Edit Blackout Window** page appears.

5. To disable the blackout window, click the **Enabled** slider.
6. To edit the blackout window settings, modify the options described in [Blackout Windows](#).
7. Click **Submit**.

Tenable.sc saves your configuration.



Delete a Blackout Window

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

For more information, see [Blackout Windows](#).

To delete a blackout window:

1. Log in to Tenable.sc via the user interface.
2. Click **Scans > Blackout Windows**.

The **Blackout Windows** page appears.

3. In the row for the blackout window you want to delete, click the  menu.

The actions menu appears.

4. Click **Delete**.

A confirmation window appears.

5. Click **Delete**.

Tenable.sc deletes the blackout window.



Tags

You can use tags in Tenable.sc to label assets, policies, credentials, or queries with a custom descriptor to improve filtering and object management. For example, you could add a tag named **East Coast Employees** to label all of your assets in that geographic area.

After you create a tag and apply it to an object, the tag is visible to all users who can view or modify that object. However, tags are not shared across object types.

For more information, see [Add a Tag](#) and [Remove or Delete a Tag](#).



Add a Tag

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

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

To add a tag:

1. Log in to Tenable.sc.
2. Navigate to the assets, policies, credentials, or queries page:
 - Click **Assets**.
 - Click **Scanning > Policies** (administrator users) or **Scans > Policies** (organizational users).
 - Click **Scanning > Credentials** (administrator users) or **Scans > Credentials** (organizational users).
 - Click **Analysis > Queries**.
3. In the row for the asset, policy, credential, or query you want to tag, click the  menu.

The actions menu appears.

4. Click **Edit**.
5. In the **Tag** drop-box, select an existing tag or type a new tag.
6. Click **Submit**.

The tag appears, applied to the asset, policy, credential, or query.



Remove or Delete a Tag

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

You can remove a tag from an asset, policy, credential, or query to stop associating that object with the tag. To completely delete a tag from Tenable.sc, you must remove the tag from all assets, policies, credentials, or queries. For more information, see [Tags](#).

To remove a tag or completely delete a tag from Tenable.sc:

1. Log in to Tenable.sc via the user interface.
2. Navigate to the assets, policies, credentials, or queries page:
 - Click **Assets**.
 - Click **Scanning > Policies** (administrator users) or **Scans > Policies** (organizational users).
 - Click **Scanning > Credentials** (administrator users) or **Scans > Credentials** (organizational users).
 - Click **Analysis > Queries**.
3. In the row for the asset, policy, credential, or query where you want to remove the tag, click the  menu.

The actions menu appears.

4. Click **Edit**.
5. In the **Tag** drop-box, remove the tag from the asset, policy, credential, or query.
6. Click **Submit**.

Tenable.sc removes the tag from the asset, policy, credential, or query.

7. (Optional) If you want to delete the tag from Tenable.sc, repeat steps 2 through 6 until you have removed all uses of the tag for the object type.

Tenable.sc deletes the tag.



Analyze Data

See the following sections to analyze and respond to Tenable.sc 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.
Event Analysis	View a table of Log Correlation Engine security event data.
Mobile Analysis	View a table of vulnerability data discovered by scanning an ActiveSync, Apple Profile Manager, AirWatch, Good, or MobileIron MDM server.
Reports	Create custom or template-based reports to export Tenable.sc data for further analysis.
Assurance Report Cards	Create ARCs to develop security program objectives and assess your organization's security posture.

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, ticketing, accepting risk, recasting risk) from some analysis tools.

If you are licensed for Lumin, you can synchronize Tenable.sc with Tenable.io Lumin to take advantage of Cyber Exposure features, as described in [Lumin Synchronization](#). For more information, contact your Tenable representative.



Dashboards

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

Administrator users can view Tenable-provided **Overview** and **LCE Overview** dashboards. For more information, see [Overview Dashboard](#) and [LCE Overview Dashboard](#).

Organizational users can configure custom or template-based *dashboards* that contain *dashboard components*, which display vulnerability, event, ticket, user, and alert data for analysis. When viewing vulnerability or event data, you can drill into the underlying data set for further evaluation.

Tip: Tenable provides many dashboard templates (e.g., the VPR Summary dashboard). For a complete index of Tenable-provided dashboard templates, see the [Tenable.sc Dashboards](#) blog.

Dashboards allow you to organize similar dashboard components to streamline your analysis. Instead of creating a single dashboard with several dozen dashboard components, you can create several dashboards that group similar dashboard components together. For example, you can create two separate dashboards to view active scanning data and passive scanning data.

Note: Dashboards display vulnerability, event, and other scan data. Tenable recommends configuring several data sources to optimize the data you see in dashboards. For more information, see [Scanning Overview](#).

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

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

To view a dashboard:

1. Log in to Tenable.sc 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.

If you are an organizational user, you can:

- Add a dashboard component to the dashboard in view, as described in [Add a Template-Based Dashboard Component](#) or [Add a Custom Dashboard Component](#).
- Manage dashboard components on the dashboard in view, as described in [Manage Dashboard Components](#).
- Edit the dashboard settings for the dashboard in view, as described in [Edit Settings for a Dashboard](#).
- Share or revoke access to the dashboard in view, as described in [Share or Revoke Access to a Dashboard](#).
- Create a report from the dashboard in view:
 - a. In the upper-right corner of the page, click the **Options** drop-down box.
 - b. Click **Send to Report**.

For more information about reports, see [Reports](#).



- Delete the dashboard in view, as described in [Delete a Dashboard](#).



Overview Dashboard

Tenable provides the **Overview** dashboard to administrator users by default. For more information, see [View a Dashboard](#).

Widget	Action
Licensing Status How close am I to hitting my license limit?	View a graph of your total license size compared to your total currently active IP addresses.
Repository Statistics How am I using my repositories?	View information about your repositories: • Name — The name of the repository. • Vuln Count — The 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. • Last Update — The date and time of the most recent scan that updated the repository data. • IP/Device Count — The number of IP addresses in the repository counting toward your Tenable.sc license. • Type — The repository type. • Data Format — The type of data stored in the repository: IPv4, IPv6, Mobile, or Agent.
System Status Is the Tenable.sc job daemon running?	• View the status of the job daemon, which powers the job queue. • To change the status of the job daemon, click Start or Stop. Tenable.sc changes the status of the job daemon.



Widget	Action
Scanner Status What is the status of my scanners?	View information about your scanners: • Name — The name of the scanner or instance. • Type — The type of connection: Passive or Active. • Status — The status of the scanner or instance.
Latest Plugins What plugins were most recently changed in a feed update?	View information about the latest plugin changes in feed updates. • ID — The plugin ID. • Name — The name of the plugin. • Family — The plugin family. • Type — The plugin type. • Date — The date and time of the feed update that contained the plugin change.



LCE Overview Dashboard

Tenable provides the **LCE Overview** dashboard to administrator users by default. For more information, see [View a Dashboard](#).

Widget	Action
LCE Status What is the status of my LCE servers?	View information about your LCE server: • Name – The name of the LCE server. • Status – The status of the LCE server.
LCE Client Status What is the status of my LCE clients?	View information about your LCE clients: • Client IP – The IP address of the LCE client. • LCE – The LCE server associated with the LCE client. • Last Update – The date and time of the most recent LCE client import to Tenable.sc. • Status – The status of the LCE client.



Set a Dashboard as Your Default Dashboard

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

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

To set a dashboard as your default dashboard:

1. Log in to Tenable.sc 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 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.sc via the user interface.
2. Click **Dashboard** > **Dashboard**.

The **Dashboards** page appears.

3. In the upper-right corner of the page, click the **Options** drop-down button.
4. Click **Add Dashboard**

The **Add Dashboard** page appears.

The **Dashboard Template** page appears.

5. In the **TemplatesCommon** 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.sc saves your configuration and the **Dashboards** page appears.

9. In the upper-right corner of the page, click the **Switch Dashboard** drop-down box.
10. Click the name of the dashboard you just created.

The page for the dashboard appears.

What to do next:

- Add dashboard components, as described in [Add a Template-Based Dashboard Component](#) or [Add a Custom Dashboard Component](#).



Add a Custom Dashboard

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

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.sc via the user interface.
2. Click **Dashboard > Dashboard**.

The **Dashboards** page appears.

3. In the upper-right corner of the page, click the **Options** drop-down button.
4. Click **Add Dashboard**

The **Add Dashboard** page appears.

The **Dashboard Template** page appears.

5. In the **CustomOther** section, click the **Advanced** tile.
6. In the **Name** box, type a name for the dashboard.
7. In the **Description** box, type a description for the dashboard.
8. In the **Layout** section, select the layout you want to use for the dashboard.
9. Click **Submit**.

Tenable.sc saves your configuration and the **Dashboards** page appears.

10. In the upper-right corner of the page, click the **Switch Dashboard** drop-down box.
11. Click the name of the dashboard you just created.

The page for the dashboard appears.

What to do next:



- Add dashboard components, as described in [Add a Template-Based Dashboard Component](#) or [Add a Custom Dashboard Component](#).



Dashboard and Component Templates

Tenable.sc 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.sc Dashboards](#) blog.

Template	Description
TemplateCommon	
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.
CustomOther (Dashboards)	
Advanced	A custom dashboard with no pre-configured settings.
Import	Import a dashboard. For more information, see Import a Dashboard .
CustomOther (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 User Role: Organizational user with appropriate permissions. For more information, see [User Roles](#).

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

To import a dashboard:

1. Log in to Tenable.sc via the user interface.
2. Click **Dashboard**.

The **Dashboards** page appears.

3. In the upper-right corner of the page, click the **Options** drop-down button.
4. Click **Add Dashboard**

The **Add Dashboard** page appears.

The **Dashboard Templates** page appears.

5. In the **CustomOther** 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.sc imports the dashboard.



Manage Dashboards

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

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

To manage dashboards:

1. Log in to Tenable.sc via the user interface.
2. Click **Dashboard** > **Dashboard**.

The **Dashboards** page appears.

3. In the upper-right corner of the page, click the **Options** drop-down button.
4. Click **Manage Dashboards**

The **Manage Dashboards** page appears.

5. To add a dashboard, click **Add**. For more information, see [Add a Template-Based Dashboard](#) or [Add a Custom Dashboard](#).
6. To filter the dashboards in the table, see [Apply a Filter](#).
7. To manage a single dashboard, click the  menu in a dashboard row.

The actions menu appears.

From this menu, you can:

- Click **View** to view details for the dashboard.
 - Click **Edit** to edit the dashboard. For more information, see .
 - Click **Share** to share or revoke access to the dashboard.
 - Click **Copy** to copy the dashboard.
 - Click **Delete** to delete the dashboard.
8. To show or hide a dashboard from the **Switch Dashboard** drop-down on the **Dashboards** page, pin or unpin the dashboard:



-  – pinned, the dashboard appears.
-  – unpinned, the dashboard does not appear.

To export the dashboard as an XML file:

- a. Click **Export**.
- b. Then, identify how you want Tenable.sc to handle object references:
 - **Remove All References** – all object references are removed, altering the definitions of the components. Importing users do not need to make any changes for components to be useable.
 - **Keep All References** – object references are kept intact. Importing users must be in the same organization and have access to all relevant objects for the components to be useable.
 - **Replace With Placeholders** – object references are removed and replaced with their respective names. Importing users see the name of the reference object, but need to replace it with an applicable object within their organization before the component is useable.

Note: Due to version-specific changes in dashboard XML file formats, exported dashboards are not always compatible for import between Tenable.sc versions.



Edit Settings for a Dashboard

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

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

To edit the settings for a dashboard:

1. Log in to Tenable.sc via the user interface.
2. Click **Dashboard** > **Dashboard**.

The **Dashboards** page appears, displaying your default dashboard.

3. If you want to switch to a different dashboard:
 - a. In the upper-right corner of the page, click the **Switch Dashboard** drop-down box.
 - b. Click the dashboard you want to view.

The dashboard appears.

4. In the upper-right corner of the page, click the **Options** drop-down box.
5. Click **Edit**.

The **Edit Dashboard** page appears.

6. Edit the **Name**, **Description**, or **Layout**.
7. Click **Submit**.

Tenable.sc saves your configuration.



Share or Revoke Access to a Dashboard

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

You can share access to a dashboard to give users in a group the ability to view the dashboard. The user's role and custom permissions determine if they can drill down into other pages with more information. For more information, see [Dashboards](#).

To share or revoke access to a dashboard:

1. Log in to Tenable.sc via the user interface.
2. Click **Dashboard** > **Dashboard**.

The **Dashboards** page appears, displaying your default dashboard.

3. If you want to switch to a different dashboard:
 - a. In the upper-right corner of the page, click the **Switch Dashboard** drop-down box.
 - b. Click the dashboard you want to view.

The dashboard appears.

4. In the upper-right corner of the page, click the **Options** drop-down box.
5. Click **Share**.

The **Share Dashboard** window appears.

6. In the box, search for and select the groups for which you want to share or revoke access.
7. Click **Submit**.

Tenable.sc saves your configuration.



Delete a Dashboard

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

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

To delete a dashboard:

1. Log in to Tenable.sc via the user interface.
2. Click **Dashboard** > **Dashboard**.

The **Dashboards** page appears, displaying your default dashboard.

3. If you want to switch to a different dashboard:
 - a. In the upper-right corner of the page, click the **Switch Dashboard** drop-down box.
 - b. Click the dashboard you want to view.

The dashboard appears.

4. In the upper-right corner of the page, click the **Options** drop-down box.
5. Click **Delete**.

A confirmation window appears.

6. Click **Delete**.

The system deletes the dashboard.



Manage Dashboard Components

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

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

To manage dashboard components:

1. Log in to Tenable.sc via the user interface.
2. Click **Dashboard** > **Dashboard**.

The **Dashboards** page appears.

To edit a dashboard component:

1. Hover over the dashboard component.
2. Click the  menu.

The actions menu appears.

3. Click **Edit**.
4. Edit the dashboard component options. For more information, see [Custom Dashboard Component Options](#).

To view the data behind a dashboard component:

1. Hover over the dashboard component.
2. Click the arrow icon.

The analysis page appears.

Note: Only dashboard components that display vulnerability analysis or event analysis data support viewing the data behind a dashboard component.

To reorder a dashboard component:

1. Click the title of a dashboard component.
2. Drag the dashboard component around the page.



To copy a dashboard component to the dashboard in view or a different dashboard:

1. Hover over the dashboard component.
2. Click the  menu.

The actions menu appears.

3. Click **Copy**.
4. In the **Name** box, edit the name for the copied dashboard component.
5. In the **Dashboard** drop-down box, click the name of the dashboard where you want to copy the dashboard component.
6. Click **Copy**.

Tenable.sc copies the dashboard component.

To refresh the dashboard component data:

1. Hover over the dashboard component.
2. Click the  menu.

The actions menu appears.

3. Click **Refresh**.

Tenable.sc refreshes the dashboard component data.

To delete the dashboard component:

1. Hover over the dashboard component.
2. Click the  menu.

The actions menu appears.

3. Click **Delete**.

A confirmation window appears.

4. Click **Delete**.

Tenable.sc deletes the dashboard component.



Add a Template-Based Dashboard Component

Required 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.sc via the user interface.
2. Click **Dashboard**.

The **Dashboards** page appears.

3. In the upper-right corner of the page, click the **Switch Dashboard** drop-down box.
4. Click the name of the dashboard for which you want to add a component.

The dashboard appears.

5. In the upper-right corner of the page, click the **Options** drop-down box.
6. Click **Add Component**.

The **Add Component** page appears.

The **Component Templates** page appears.

7. In the **TemplatesCommon** 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.sc saves your configuration and the **Dashboards** page appears.



Add a Custom Dashboard Component

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

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](#).

Before you begin:

- Add a dashboard, as described in [Add a Template-Based Dashboard](#), [Add a Custom Dashboard](#), or [Import a Dashboard](#).

To add a custom dashboard component to a dashboard:

1. Log in to Tenable.sc via the user interface.
2. Click **Dashboard**.

The **Dashboards** page appears.

3. In the upper-right corner of the page, click the **Switch Dashboard** drop-down box.
4. Click the name of the dashboard for which you want to add a component.

The dashboard page appears.

5. In the upper-right corner of the page, click the **Options** drop-down box.
6. Click **Add Component**.

The **Add Component** page appears.

The **Component Templates** page appears.

7. In the **CustomOther** 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.sc 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.sc 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](#)

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.	--
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	Daily



Option	Description	Default
	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.	

Table Component Options

Option	Description	Default
Data		
Type	The type of data: Vulnerability , Event , Mobile , User , Ticket , or Alert .	Vulnerability
Query	Predefined query used to further narrow down the data source options. If a query does not exist or is not desired, it may be left unselected. The query may be used as is or as a template on which to base the Filters option.	--
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.sc can use only active event data for event-based components.	Cumulative
Tool	The analysis tool to use for creating the chart. For more information, see Vulnerability Analysis Tools and Event Analysis Tools .	Vulnerability Summary
Filters	Additional filters to use on the data source. For more information, see Filters .	--



Option	Description	Default
Display		
Results Displayed	The number of displayed results. You can choose to display up to 999 results. 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.	10
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.sc uses to sort the results.	Plugin ID
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.	--

Bar Chart Component Options

Option	Description	Default
Data		
Type	The type of data: Vulnerability, Event, Mobile, or Ticket.	Vulnerability
Query	Predefined query used to further narrow down the data source options. If a query does not exist or is not desired, it may be left unselected. The query may be used as is or as a template on which to base the Filters option.	--
Source	(If Type is Vulnerability or Event) Specifies the data	Cumulative



Option	Description	Default
	source. For vulnerability data, select Cumulative or Mitigated . For event data, the data source is Active . Tenable.sc can use only active event data for event-based components.	
Tool	The analysis tool to use for creating the chart. For more information, see Vulnerability Analysis Tools and Event Analysis Tools .	Vulnerability Summary
Filters	Additional filters to use on the data source. For more information, see Filters .	--
Display		
Results Displayed	The number of displayed results. You can choose to display up to 100 results.	10
Sort Column	(If Type is Vulnerability or Ticket) The column Tenable.sc uses to sort the results.	Plugin ID
Sort Direction	(If Type is Vulnerability or Ticket) The sort direction: Descending or Ascending .	Descending
Display Column	The columns to display in the component output.	--

Pie Chart Component Options

Option	Description	Default
Data		
Type	The type of data: Vulnerability , Event , Mobile , or Ticket .	Vulnerability
Query	Predefined query used to further narrow down the data source options. If a query does not exist or is not desired, it may be left unselected. The query may be used as is or	--



Option	Description	Default
	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.sc can use only active event data for event-based components.	Cumulative
Tool	The analysis tool to use for creating the chart. For more information, see Vulnerability Analysis Tools and Event Analysis Tools .	Vulnerability Summary
Filters	Additional filters to use on the data source. For more information, see Filters .	--
Display		
Results Displayed	The number of displayed results.	10
Sort Column	The column Tenable.sc uses to sort the results.	Plugin ID
Sort Direction	The sort direction: Descending or Ascending .	Descending
Display Column	The columns to display in the component output.	--

Matrix Component Options

For information about configuring matrix components and to download samples, visit the [Tenable.sc 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, or alert 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.sc 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.sc stops reviewing rules for the cell. If none of the added rules match, Tenable.sc 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.sc supports matrices from 1x1 to 10x10. Click Generate Cells create a blank matrix with customizable cells.
 gear icon	Click the  gear 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.sc deletes the row or column. • To copy the row or column, click Copy. Tenable.sc copies the row or column.
 pencil	Click the  pencil icon inside a cell to configure rules for the cell. For more inform-



Option	Action
icon	ation, see Matrix Component Query Options .

Matrix Component Query Options

Option	Description	Default
Data		
Data Type	The type of data: Vulnerability, Mobile, Event, User, Alert, or Ticket. 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.sc can use only active event data for event-based components.	Cumulative
Filters	(If Type is Count) Additional filters to use on the data source. For more information, see Filters .	--
Numerator Filters	(If Type is Ratio) The filters to apply to the ratio numerator. For more information, see Filters .	--
Denominator Filters	(If Type is Ratio) The filters to apply to the ratio denominator. For more information, see Filters .	--
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.	--



Option	Description	Default
	Quantities: Less than or equal to, Greater than or equal to, Exactly, or Not Equal to. Query values: Events, Hosts, Vulnerabilities, Ports, Devices, Users, Alerts, or Tickets. Note: The available query values depend on the Data Type.	
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.	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 24 Hours



Option	Description	Default
	• 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.	
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 Event. 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
Query	Predefined query used to further narrow down the data source options. If a query does not exist or is not desired, it may be left unselected. The query may be used as is or as a template on which to base the Filters option.	--



Filters	Additional filters to use on the data source. For more information, see Filters .	--
Display		
Series Data	Data to display in the chart: Total, Info, Low, Medium, High, or Critical .	All



Configure a Simple Matrix Dashboard Component

Required 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.



Add Matrix Component

Name*

Executive 7 Day - Exploitable Vulnerability

Description

Percentages of hosts with exploitable vulnerabilities over the last 7 day and the frameworks that can be used to exploit them.

Cells

Size*

5

Columns x

3

Rows

[Generate Cells](#)

[Submit](#)

[Cancel](#)

For example, 5 columns and 3 rows.

- Click **Generate Cells**.

The matrix editor appears.

- Next to the header label, click the  menu.

The actions menu appears.

- Click **Edit Header**.

- Type a **Label** for the column or row header.

- Click **Submit**.

The matrix editor appears, with the new header label displayed.



Cells

	Exploit %	Metasploit	Core Impact	Canvas	Malware
Critical					
High					
Medium					

Submit

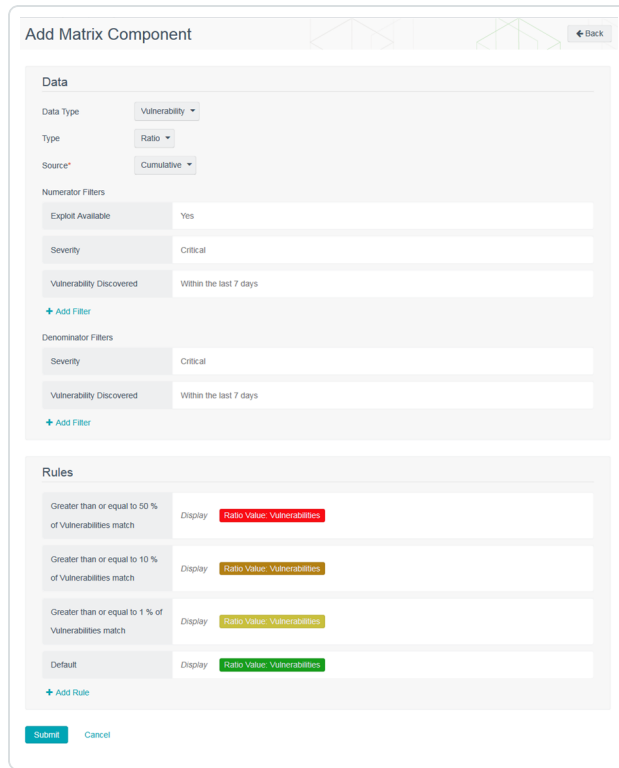
Cancel

- Repeat the header label steps for the other header cells.
- Hover over the body cells and click the edit icon.

The **Add Matrix Component** page appears.

- Customize the matrix component options.

For example, this matrix component displays Vulnerability data by a ratio from the Cumulative database. The numerator filters are looking for vulnerabilities that have an exploit available with a Critical severity and were discovered within the last 7 days. The Denominator filters are for vulnerabilities that have a Critical severity and were discovered within the last 7 days. The rules are looking for percentages of the vulnerabilities that match and designate the ratio value with the corresponding color based on the percentages found.



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.



Cells

	Exploit %	Metasploit	Core Impact	Canvas	Malware
Critical					
High					
Medium					

Submit

Cancel

13. Click **Submit**.

The matrix element appears.



Scan Results

The **Scan Results** page displays scan results and statuses from active scans, agent scans, and agent synchronization jobs .

Note: Tenable.sc does not include all agent scans in the scan results table. If an agent scan imports scan results identical to the previous agent scan, Tenable.sc omits the most recent agent scan from the scan results table.

Note: If you added the parent node of a Nessus Manager cluster as a scanner in Tenable.sc, Tenable.sc displays scan results for all child nodes. For more information, see [Clustering](#) in the *Nessus User Guide*.

Note: For each agent synchronization job result for a child node, Tenable.sc imports a metadata record containing no vulnerability data. This metadata record appears as a second result on the **Scan Results** page. To prevent Tenable.sc from importing the metadata file, configure and launch agent scans from Tenable.sc, as described in [Agent Scans](#).

For more information, see [Manage Scan Results](#) and [Scan Result Statuses](#).



Scan Result Statuses

You can view the scan status and the import status for all scan results, as described in [View Scan Result Details](#).

- [Scan Status](#)
- [Import Status](#)

Scan Status

The scan status specifies the status of the scan.

Status	Description
Active Scans	
Queued	The scan is queued.
Preparing	Tenable.sc is preparing to run the scan.
Resolving Hostnames	Tenable.sc is resolving hostnames before running the scan.
Verifying Targets	Tenable.sc is verifying targets before running the scan.
Initializing Scanners	Tenable.sc is initializing scanners before running the scan.
Running	The scan is running.
Pausing	You paused the scan and Tenable.sc is pausing the scan.
Paused	The scan is paused.
Resuming	You resumed the scan and Tenable.sc is resuming the scan.
Stopping	Tenable.sc is stopping the scan.
Completed	The scan finished successfully.
Partial	The scan finished and some results are available.
Error	The scan did not finish.



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.

Import Status

The scan status specifies the status of the scan result import to Tenable.sc.

Status	Description
Active and Agent Scans	
No Results	The scan finished successfully but yielded no results.
Pending	Tenable.sc is preparing to start the import.
Importing	Tenable.sc is importing the scan result data.
Finished	The import finished successfully.
Blocked	Tenable.sc 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.
Error	The import did not finish.



Manage Scan Results

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

Depending on the state of a scan result, you can perform different management actions (e.g., you cannot download results for a scan with errors).

For more information, see [Scan Results](#).

To manage scan results:

1. Log in to Tenable.sc via the user interface.
2. Click **Scans > Scan Results**.

The **Scan Results** page appears.

3. Manage the results:

To filter the scan results:

- Click the filter icon.

Filters allow you to view only desired scan results. Filter parameters include the **Name**, **Group**, **Owner**, **Scan Policy**, **Status**, **Completion Time**, **Access**, and **Type**.

To remove all filters:

- Under the filter options, click **Clear Filters**.

Note: To return to the default filter for your user account, refresh your browser window. The number in grey next to the filter displays how many filters are currently in use.

To view a set of scan results:

- a. In the row for the scan, click the  menu.

The actions menu appears.

- b. Select **Browse**.

The Vulnerability Summary analysis tool appears, populated with data from the scan.

To view scan result details for a set of scan results:



- a. In the row for the scan, click the  menu.

The actions menu appears.

- b. Click **View**.

The **View Scan Result** page appears. For more information, see [Scan Result Details](#).

To download the results of a scan:

- a. In the row for the scan, click the  menu.

The actions menu appears.

- b. Select **Download**.

Tip: On a standard scan, you can download a Nessus results file. If the scan contains SCAP results, you can use an additional option to download the SCAP results.

To manually import scans listed on the scan results page:

- a. In the row for the scan, click the  menu.

The actions menu appears.

- b. Select **Import**.

Tip: This option is useful for cases where a scan may have not fully imported after completion. For example, if a scan was blocked because importing it would have exceeded the licensed IP address count, you can increase the IP address count, then import the scan results previously not imported.

To share scan results with other users:

- a. In the row for the scan, click the  menu.

The actions menu appears.

- b. Select **Copy**.

Selecting a **Group** from the drop-down box displays a list of users from that group. You can select one or more users from the list.

To send a copy of the scan results to users without access to Tenable.sc:



- a. In the row for the scan, click the  menu.

The actions menu appears.

- b. Select **Email**.

To generate a report for the scan results based off a preconfigured report:

- a. In the row for the scan, click the  menu.

The actions menu appears.

- b. Select **Send to Report**.

Tenable.sc sends the scan results to a report.

To upload Nessus scan results performed by other systems:

- See [Upload Scan Results](#).

To pause or resume a running scan:

- In the row for the scan, click the pause or play button, as described in [Start or Pause a Scan](#).

To delete a set of scan results from Tenable.sc:

- a. In the row for the scan, click the  menu.

The actions menu appears.

- b. Select **Delete**.

Tenable.sc deletes the scan results.



View Scan Results

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

For more information, see [Scan Results](#).

Note: Tenable.sc does not include all agent scans in the scan results table. If an agent scan imports scan results identical to the previous agent scan, Tenable.sc omits the most recent agent scan from the scan results table.

Note: If you added the parent node of a Nessus Manager cluster as a scanner in Tenable.sc, Tenable.sc displays scan results for all child nodes. For more information, see [Clustering](#) in the *Nessus User Guide*.

Note: For each agent synchronization job result for a child node, Tenable.sc imports a metadata record containing no vulnerability data. This metadata record appears as a second result on the **Scan Results** page. To prevent Tenable.sc from importing the metadata file, configure and launch agent scans from Tenable.sc, as described in [Agent Scans](#).

To view a list of scan results:

1. Log in to Tenable.sc via the user interface.
2. Click **Scans > Scan Results**.

The **Scan Results** page appears.

3. View details about each scan result.
 - **Name** — The name for the scan associated with the result.
 - **Type** — The type of scan that generated the scan result.
 - **Scan Policy Plugins** — The name of the scan policy that generated the scan result.
 - **Scanned IPs** — The number of IP addresses scanned.
 - **Group** — The group associated with the scan.
 - **Owner** — The username for the user who added the scan.
 - **Duration** — The total time elapsed while running the scan.



- **Import Time** — The date and time Tenable.sc completed the scan result import.
- **Status** — The status of the scan that generated the scan result. For more information, see [Scan Status](#).

4. To view additional details for a scan result, see [View Scan Result Details](#).



View Scan Result Details

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

You can view details for any scan result. For more information, see [Scan Results](#).

To view scan result details:

1. Log in to Tenable.sc via the user interface.
2. Click **Scans > Scan Results**.

The **Scan Results** page appears.

3. In the row for the scan result, click the  menu.

The actions menu appears.

4. Click **View**.

The **View Scan Result** page appears.

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. • 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.



Section	Action
	• Start Time – The date and time Tenable.sc started the scan. • Finish Time – The date and time Tenable.sc 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.sc started the scan result import. • Import Finish – The date and time Tenable.sc 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.
Tenable.io Syn- chronization Data	View synchronization summary data: • Status – The status of the Lumin synchronization containing this scan result data: • Not Synced – The repository containing this scan result data is not configured for Lumin synchronization. • Syncing – The Lumin synchronization containing this scan result data is in progress.



Section	Action
	• Finished – The most recent synchronization that included this scan result data succeeded. • Error – An error occurred. For more information, see View Lumin Data Synchronization Logs. • Start Time – The date and time Tenable.sc started the most recent transfer of data to Tenable.io. • Finish Time – The date and time Tenable.sc finished the most recent transfer of data to Tenable.io. • Duration – The total time elapsed during the most recent transfer of data to Tenable.io. • Details – If the Status is Error, details about the error. For more information about Lumin synchronization, see Lumin Synchronization.



Upload Scan Results

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

You can upload active or agent scan results from scans performed by other systems. Tenable.sc supports either raw (.nessus) or compressed (.zip) files, with one .nessus file per archive before uploading. This allows you to import scan results from scans run in remote locations without network connectivity to Tenable.sc.

Note: To upload files greater than 300 MB to Tenable.sc, you must modify `upload_max_filesize` in `/opt/sc/support/etc/php.ini` to accommodate the larger uploads.

Scan Result-Repository Incompatibility

Caution: Tenable does not recommend importing scan results to incompatible repositories since data may be omitted.

If you upload agent scan results to a non-agent repository, Tenable.sc omits all vulnerabilities without **IP Address** data for the host. Non-agent repositories cannot uniquely identify hosts without **IP Address** data for the host.

If you upload non-agent scan results to an agent repository, Tenable.sc omits all vulnerabilities without **Agent ID** data for the host. Agent repositories cannot uniquely identify hosts without **Agent ID** data for the host.

To upload scan results:

1. Log in to Tenable.sc via the user interface.
2. Click **Scans > Scan Results**.

The **Scan Results** page appears.

3. Click **Upload Scan Results**.
4. In the **Scan File** option, click **Choose File**.

The file uploads to Tenable.sc.

5. In the **Import Repository** drop-down box, select a repository.



6. If you selected an IPv4 or IPv6 repository, enable or disable the **Advanced** options: **Track hosts which have been issued new IP address**, **Scan Virtual Hosts**, and **Immediately remove vulnerabilities from scanned hosts that do not reply**.

For more information about the advanced options, see [Active Scan Settings](#).

7. Click **Submit**.

Tenable.sc saves your configuration.



Solutions Analysis

Tenable provides recommended solutions for all vulnerabilities on your network. You can perform the recommended action in a solution to lower the risk on your network.

For more information, see:

- [View Solutions](#)
- [View Solution Details](#)



View Solutions

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

You can use the **Solutions** page to view solutions for specific assets on your network or drill into solution details.

To view solutions for assets on your network:

1. Log in to Tenable.sc via the user interface.
2. Click **Solutions**.

The **Solutions** page appears.

3. To filter the solutions in the table by an asset list, in the **Targeted Assets** drop-down box, click an asset list name.

The system refreshes the page and filters the table by the asset list you selected. For more information about asset lists, see [Assets](#).

4. View information about each solution.
 - **Solution** – A description for the solution.
 - **Risk Reduction** – The percent you would reduce your risk by addressing the vulnerability in the solution. Tenable.sc calculates the risk reduction percentage by dividing the score of the vulnerabilities in the solution by the score of all of the vulnerabilities on your network.
 - **Hosts Affected** – The number of devices affected by the solution.
 - **Vulnerabilities** – The number of vulnerability instances included in the solution.

Tip: A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

- **VPR** – The highest VPR for a vulnerability included in the solution.
- **CVSSv3 Base Score** – The highest CVSSv3 score for a vulnerability included in the solution. If only CVSSv2 is available, the column is blank.



5. To view details for a solution, click a row.

The **Solution Details** page appears. For more information, see [Solution Details](#).



View Solution Details

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

You can use the **Solution Details** page to view details for a specific solution.

To view details for a specific solution:

1. Log in to Tenable.sc 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. 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.



Section	Action
	• Plugin — The plugin ID. • Hosts Affected — The number of devices affected by the solution. • VPR — The VPR for the vulnerability. • CVSSv3 Base Score — The CVSSv3 score for the vulnerability included in the solution. If only CVSSv2 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. • DNS — The DNS name, if known. • OS CPE — The operating system common platform enumeration (CPE) name. • Repository — The repository name where device's scan data is stored. A device appears in multiple rows if the device's scan data is stored in multiple repositories.



Vulnerability Analysis

The **Vulnerability Analysis** page displays vulnerabilities from either the cumulative or mitigated vulnerability database. For more information, see [Cumulative vs. Mitigated Vulnerabilities](#).

Note: If multiple vulnerabilities share the same **IP Address** or **Agent ID** data, Tenable.sc assumes they are from the same host.

To perform a common type of vulnerability analysis, see [View Vulnerabilities by Plugin](#) or [View Vulnerabilities by Host](#).

To view a specific vulnerability analysis tool, see [Vulnerability Analysis Tools](#).



Cumulative vs. Mitigated Vulnerabilities

Tenable.sc stores vulnerabilities in two databases: the cumulative database and the mitigated database. You can choose to view cumulative vulnerabilities or mitigated vulnerabilities in any vulnerability analysis tool. For more information, see [View Cumulative or Mitigated Vulnerabilities](#).

Cumulative Vulnerabilities

The cumulative database contains currently vulnerable vulnerabilities, including those that have been recasted, accepted, or previously mitigated.

Mitigated Vulnerabilities

The mitigated database contains vulnerabilities that Tenable.sc determines are not vulnerable, based on the scan definition, the results of the scan, the current state of the cumulative view, and authentication information.

A vulnerability is mitigated if:

- The IP address of the vulnerability was in the target list of the scan.
- The plugin ID of the vulnerability was in the list of scanned plugins.
- The port of the vulnerability was in the list of scanned ports.
- The vulnerability with that IP address/port/plugin ID combination was not in the scan result.

To start, the vulnerability must be present in the cumulative view to be considered for mitigation. The import process then looks at each vulnerability in the import repository. The import process also verifies that authentication was successful before mitigating any local check vulnerabilities that meet the above criteria.

Note: Mitigation logic works with scans using policies defined by templates, advanced policies, and remediation scans. These policies are set up to take advantage of this new mitigation logic.

For more information about mitigation, see the [knowledge base](#) article.



View Cumulative or Mitigated Vulnerabilities

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

For general information about cumulative vulnerabilities and mitigated vulnerabilities, see [Cumulative vs. Mitigated Vulnerabilities](#).

To switch between viewing mitigated or cumulative vulnerabilities:

1. Log in to Tenable.sc via the user interface.
2. Click **Analysis > Vulnerabilities**.

The **Vulnerability Analysis** page appears.

3. In the upper-right corner, click the **Options** drop-down menu.

The actions menu appears.

4. Click **Switch to Mitigated** or **Switch to Cumulative**.

The page updates to display data from the mitigated or cumulative vulnerability database.



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 **Vulnerability Analysis** 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 CVSSv2 score

Tenable.sc analysis pages provide summary information about vulnerabilities using the following CVSS categories.

Severity	CVSSv2 Range
Critical	The plugin's highest vulnerability CVSSv2 score is 10.0.
High	The plugin's highest vulnerability CVSSv2 score is between 7.0 and 9.9.
Medium	The plugin's highest vulnerability CVSSv2 score is between 4.0 and 6.9.
Low	The plugin's highest vulnerability CVSSv2 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.

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 in the National Vulnerability Database (NVD) (e.g., many vulnerabilities with the **Info** severity) do not receive a VPR. Tenable recommends remediating these vulnerabilities according to their CVSS-based severity.

Note: You cannot edit VPR values.

Tenable.sc provides new and updated VPR values through the Tenable.sc feed. For more information, see [Edit Plugin and Feed Schedules](#).

Tenable recommends resolving vulnerabilities with the highest VPRs first. You can view VPR scores and summary data in:

- The Tenable-provided **Vulnerability Priority Rating (VPR) Summary** dashboard, described in [Dashboards](#).
- The **Vulnerability Summary**, **Vulnerability List**, and **Vulnerability Detail List** tools, described in [View Vulnerabilities by Plugin](#).

VPR Key Drivers

You can view the following key drivers to explain a vulnerability's VPR.

Note: Tenable does not customize these values for your organization; VPR key drivers reflect a vulnerability's global threat landscape.

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.sc 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 (0-730) since a threat event occurred for the vulnerability.

Threat Event Examples

Common threat events include:

- An exploit of the vulnerability
- A posting of the vulnerability exploit code in a public repository
- A discussion of the vulnerability in mainstream media
- Security research about the vulnerability
- A discussion of the vulnerability on social media channels



- A discussion of the vulnerability on the dark web and underground
- A discussion of the vulnerability on hacker forums



Vulnerability Analysis Tools

On the **Vulnerability Analysis** page, you can use the drop-down box to select the vulnerability analysis tool you want to view.

To perform a common type of vulnerability analysis, see [View Vulnerabilities by Plugin](#) or [View Vulnerabilities by Host](#).

Analysis Tool	Description
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.
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.
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. 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.



Analysis Tool	Description
	You can click a count to view the Vulnerability Summary tool, filtered by the CCE vulnerability you selected.
CVE Summary	This view groups vulnerabilities based on their CVE ID, Hosts Total, and vulnerability count.
DNS Name Summary	Tenable.sc includes the ability to summarize information by vulnerable DNS name. The DNS Name Summary lists the matching hostnames, the repository, vulnerability count, and a breakdown of the individual severity counts. You can click a DNS name to view the Vulnerability List tool, filtered by the DNS name you selected.
List Mail Clients	Tenable.sc uses NNM to determine a unique list of email clients. The list contains the email client name, count of detections, and the detection method. You can click a count to view the IP Summary tool, filtered by the email client you selected.
List OS	Tenable.sc 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.sc 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 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 detec-



Analysis Tool	Description
	tions, 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 Software	Tenable.sc processes information from scans and creates a summary of unique software packages discovered. The software name, 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 Web Clients	Tenable.sc understands NNM plugin ID 1735, which passively detects the web client in use. This tool lists the unique web clients detected. The list contains the user-agents, count of detections, and the detection method. You can click a count to view the 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.
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	This tool charts the Nessus, NNM, or Event plugin family as well as their



Analysis Tool	Description
Summary	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 addressing the vulnerability in the solution. Tenable.sc calculates the risk reduction percentage by dividing the score of the vulnerabilities in the solution by the score of all of the vulnerabilities on your network. • Hosts Affected – The number of unique hosts that would be affected by performing the remediation action. • Vulnerabilities – The count of vulnerabilities (Nessus plugins) that would be remediated by performing the remediation action. • Score – This is calculated by adding up the score for each vul-



Analysis Tool	Description
	nerability 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 (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 Responsibility Summary	This displays a list of the users who are assigned responsibility for the vulnerability based on the user's assigned asset list. Multiple users with the same responsibility are displayed on the same line. Users without any assigned responsibilities are not displayed in the list. Tenable.sc populates this list after you assign an asset to a user account.
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.



Analysis Tool	Description
	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 constructing filters, see [Filters](#).

Filter Component	Availability	Description
Accept Risk	Cumulative View	Display vulnerabilities based on their Accepted Risk workflow status. Available choices include Accepted Risk or Non-Accepted Risk . Choosing both options displays all vulnerabilities regardless of acceptance status.
Address	All	This filter specifies an IPv4 or IPv6 address, range, or CIDR block to limit the viewed vulnerabilities. For example, entering <i>198.51.100.28/24</i> and/or <i>2001:DB8::/32</i> limits any of the web tools to only show vulnerability data from the selected network(s). Addresses can be comma separated or 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.ot assets that may not have an IP address. For more information, see Tenable.ot Instances.
Application CPE	All	Allows a text string search to match against available CPEs. The filter may be



Filter Component	Availability	Description
		set to search based on a contains , Exact Match , or Regex Filter filter. The Regex Filter is based on Perl-compatible regular expressions (PCRE).
Asset	All	This filter displays systems from the assets you select. If more than one asset contains the systems from the primary asset (i.e., there is an 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.
Audit File	All	This filter displays vulnerabilities detected when a scan was performed using the chosen .audit file.
CCE ID	All	Displays results matching the entered CCE ID.
CVE ID	All	Displays vulnerabilities based on one or more CVE IDs. Type multiple IDs as a comma-separated list (e.g., CVE-2011-3348,CVE-2011-3268,CVE-2011-3267).
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



Filter Component	Availability	Description
		Common Vulnerability Scoring System version 3 (CVSS v3) score range.
CVSS v3 Vector	All	Filters results based on a search against the CVSS v3 vector information.
Cross References	All	Filters results based on a search against the cross reference information in a vulnerability.
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 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 IAVM IDs. Type multiple IDs as a comma-separated list (e.g., 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	Display vulnerabilities for a specific mit-



Filter Component	Availability	Description
		igation 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.
Output Assets	Asset Summary Analysis Tool	This filter displays only the desired asset list systems.
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



Filter Component	Availability	Description
		• Current Month • Last Month • Current Quarter (during the current calendar year quarter) • Last Quarter (during the previous calendar year quarter) • Custom Range (during a specific range you specify) • Explicit (at a specific time you specify)
Plugin Family	All	This filter chooses a Nessus or NNM plugin family. Only vulnerabilities from that family display.
Plugin ID	All	Type the plugin ID desired or range based on a plugin ID. Available operators are equal to (=), not equal to (!=), greater than or equal (>=) 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



Filter Component	Availability	Description
		• 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) • Custom Range (during a specific range you specify) • 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. Using the Regex Match option regex options may be used to filter on the Plugin Name.



Filter Component	Availability	Description
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 quarter) • Last Quarter (during the previous calendar year quarter) • 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,



Filter Component	Availability	Description
		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	Display vulnerabilities based on their Recast Risk workflow status. Available choices include Recast Risk or Non-Recast Risk . Choosing both options displays all vulnerabilities regardless of recast risk status.
Repositories	All	Display vulnerabilities from the chosen repositories.
STIG Severity	All	Display vulnerabilities with the chosen STIG severity in the plugins database.
Scan Policy Plugins	All	Display vulnerabilities found by the currently enabled plugins in the scan policy. For more information, see Plugins Options .
Severity	All	Displays vulnerabilities with the selected severity. For more information, see CVSS vs. VPR .
Users	All	Allows selection of one or more users



Filter Component	Availability	Description
		who are responsible for the vulnerabilities.
Vulnerability Discovered	All	Tenable.sc 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) • Custom Range (during a specific range you specify) • Explicit (at a specific time you specify) Note: The discovery date is based on when the vulnerability was first imported into Tenable.sc. For NNM, this date does not match the exact vulnerability discovery time as there is normally a lag between the



Filter Component	Availability	Description
		time that NNM 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 Nessus, LCE, or NNM: • 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) • Custom Range (during a specific range you specify) • Explicit (at a specific time you specify)



Filter Component	Availability	Description
		Note: The observation date is based on when the vulnerability was most recently imported into Tenable.sc. For NNM, this date does not match the exact vulnerability discovery as there is normally a lag between the time that NNM discovers a vulnerability and the import occurs.
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) • Custom Range (during a specific range you specify) • Explicit (at a specific time you specify)
Vulnerability Priority Rating	All	Displays vulnerabilities within the chosen VPR range. For more information, see



Filter Component	Availability	Description
(VPR)		CVSS vs. VPR. Tip: The Vulnerability Analysis 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: • 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) • Custom Range (during a specific range you specify) • Explicit (at a specific time you specify)



Filter Component	Availability	Description
Vulnerability Text	All	Displays vulnerabilities containing the entered text (e.g., php 5.3) or regex search term.



View Vulnerabilities by Host

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

You can drill into analysis views, filtering by host, to view vulnerabilities and vulnerability instances on a host.

To view vulnerabilities and vulnerability instances associated with a host:

1. Log in to Tenable.sc via the user interface.
2. Click **Analysis > Vulnerabilities**.

The **Vulnerability Analysis** page appears.

3. In the drop-down box, click **IP Summary**.

The **IP Summary** tool appears.

4. Filter the tool to locate the host where you want to view vulnerability instance details, as described in [Filters](#) and [Vulnerability Analysis Filter Components](#).
5. Click the row for the vulnerability instance where you want to view vulnerability instance details.

The **Vulnerability List** tool appears, filtered by the vulnerability instance you selected.

In this tool, you can:

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 the default display columns for the view. • Set this view as your default view.



	• Switch between viewing cumulative vulnerabilities or mitigated vulnerabilities, as described in View Cumulative or Mitigated Vulnerabilities.
Filters side bar	Apply a filter, as described in Apply a Filter and Vulnerability Analysis Filter Components .
Vulnerability row	• Click the Plugin ID ⓘ to view the plugin details associated with the vulnerability, as described in View Plugin Details. • Click the IP Address ⓘ to view the host details for the vulnerability, as described in View Host Details. • Click the row to view the vulnerability instance details in the Vulnerability Detail List tool, as described in View Vulnerability Instance Details. Tip: A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.



View Vulnerabilities by Plugin

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

You can drill into analysis views, filtering by plugin, to view vulnerabilities and vulnerability instances related to that plugin.

To view vulnerabilities and vulnerability instances associated with a plugin:

1. Log in to Tenable.sc via the user interface.
2. Click **Analysis > Vulnerabilities**.

The **Vulnerability Analysis** page appears.

3. In the drop-down box, click **Vulnerability Summary**.

The **Vulnerability Summary** tool appears.

In this tool, you can:

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 the default display columns for the view. • Set this view as your default view. • Switch between viewing cumulative vulnerabilities or mitigated vulnerabilities, as described in View Cumulative or Mitigated Vulnerabilities.
Table header	Click ▼ or ▲ next to a column name to sort the table by that column. Not all columns support sorting.



Filters side bar	Apply a filter, as described in Apply a Filter and Vulnerability Analysis Filter Components .
Plugin row	- Click the Plugin ID  to view the plugin details for the plugin, as described in View Plugin Details. - Click the row to view the vulnerability details in the Vulnerability List tool.
Plugin row  menu	- View the Asset Summary tool, DNS Summary tool, or IP Summary tool for the plugin. - 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.

- 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:

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 the default display columns for the view. - Set this view as your default view.



	• Switch between viewing cumulative vulnerabilities or mitigated vulnerabilities, as described in View Cumulative or Mitigated Vulnerabilities.
Filters side bar	Apply a filter, as described in Apply a Filter and Vulnerability Analysis Filter Components .
Vulnerability row	• Click the Plugin ID ⓘ to view the plugin details associated with the vulnerability, as described in View Plugin Details. • Click the IP Address ⓘ to view the host details for the vulnerability, as described in View Host Details. • Click the row to view the vulnerability instance details in the Vulnerability Detail List tool, as described in View Vulnerability Instance Details. Tip: A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.



View Vulnerability Instance Details

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

You can drill into analysis views to view details for a specific instance of a vulnerability found on your network.

Tip: A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

To view vulnerability instance details:

1. Log in to Tenable.sc via the user interface.
2. Click **Analysis > Vulnerabilities**.

The **Vulnerability Analysis** page appears.

3. In the drop-down box, click **Vulnerability Details List**.

The **Vulnerability Details List** tool appears.

In this tool, you can:

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.
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. Note: The discovery date is based on when the vulnerability was first imported into Tenable.sc. For NNM, this date does not match the exact vulnerability discovery time as there is normally a lag between the time that NNM discovers a vulnerability and the import occurs. 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.
Host Information	View details about the asset.
Risk Information	View metrics (e.g., CVSS score, VPR, etc.) about the risk associated with the vulnerability.
Exploit Information	View details about the exploit.



Plugin Details	View details about the plugin.
VPR Key Drivers	View the key drivers Tenable used to calculate the VPR score. For more information, see 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.



View Host Details

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

You can drill into analysis views to view details for a specific host on your network.

To view host details:

1. Log in to Tenable.sc via the user interface.
2. Click **Analysis > Vulnerabilities**.

The **Vulnerability Analysis** page appears.

3. In the drop-down box, click **Vulnerability List**.

The **Vulnerability List** tool appears.

4. In the **IP Address** column, click  to view host details for a specific vulnerability instance.

Tip: A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

The host details panel appears.

In this panel, you can:

Section	Actions
System Information	View information about the host system.
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 Assets .



View Plugin Details

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

You can drill into analysis views to view details for a specific instance of a vulnerability found on your network.

Tip: A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

To view plugin details:

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

2. Click **Analysis > Vulnerabilities**.

The **Vulnerability Analysis** page appears.

3. In the drop-down box, click **Vulnerability Summary**.

The **Vulnerability Summary** tool appears.

4. In the **Plugin ID** column, click ⓘ 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.



Export Vulnerability Data

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

You can export data from the **Vulnerability Analysis** page as a .csv or a .pdf file.

To export data from the Vulnerability Analysis page:

1. Log in to Tenable.sc via the user interface.
2. Click **Analysis > Vulnerabilities**.

The **Vulnerability Analysis** page appears.

3. In the upper-right corner, click the **Options** drop-down box.
4. Click **Export as CSV** or **Export as PDF**.

Note: If the record count (rows displayed) of any CSV export is greater than 1,000, Tenable.sc prompts you for the name of the CSV report you want to generate. After generation, you can download the report from the **Report Results** page.

5. Select or clear the check boxes to indicate which columns you want to appear in the exported file.
6. Click **Submit**.

Tenable.sc exports the vulnerability data.



Event Analysis

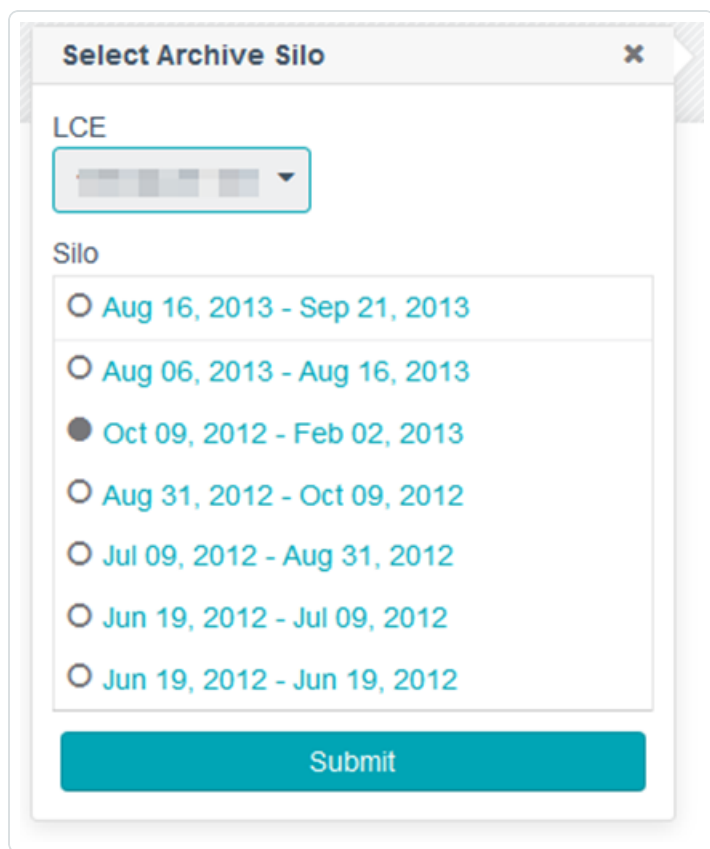
The Events display page contains an aggregation of security events from Log Correlation Engine. Events can be viewed in a list format with options similar to the Vulnerability interface.

Raw Syslog Events

Tenable.sc's event filters includes a **Syslog Test** option to narrow down the scope of a set of events, and supports the use of keyword searches for active filters. In the example above, a mix of collapsed and expanded events are seen. Selecting the **Collapse All** or **Expand All** option from the top right **Options** drop-down menu will perform that action for all of the results en masse. By selecting a particular event and clicking on the **+** or **-** icon on the right side of the event will expand or collapse that one event.

Active vs. Archived

In the **Options** drop-down menu the view can be switched between the **Active** and **Archived** data. This selection determines whether the displayed events are pulled from the active or an archived event database. The Active view is the default that displays all currently active events. The Archived view prompts for the selection of the LCE and an Archive Silo from which the event data will be displayed. In the example below, the LCE and Silo date range are displayed to help the user choose the correct archive data for analysis.

A dialog box titled "Select Archive Silo" with a close button (X) in the top right corner. Inside the dialog, there is a section labeled "LCE" with a dropdown menu showing a blurred selection. Below this is a section labeled "Silo" containing a list of date ranges, each preceded by a radio button. The selected option is "Oct 09, 2012 - Feb 02, 2013", indicated by a filled radio button. The other options are "Aug 16, 2013 - Sep 21, 2013", "Aug 06, 2013 - Aug 16, 2013", "Aug 31, 2012 - Oct 09, 2012", "Jul 09, 2012 - Aug 31, 2012", "Jun 19, 2012 - Jul 09, 2012", and "Jun 19, 2012 - Jun 19, 2012". At the bottom of the dialog is a teal "Submit" button.

Select Archive Silo

LCE

Silo

- ☐ Aug 16, 2013 - Sep 21, 2013
- ☐ Aug 06, 2013 - Aug 16, 2013
- ☒ Oct 09, 2012 - Feb 02, 2013
- ☐ Aug 31, 2012 - Oct 09, 2012
- ☐ Jul 09, 2012 - Aug 31, 2012
- ☐ Jun 19, 2012 - Jul 09, 2012
- ☐ Jun 19, 2012 - Jun 19, 2012

Submit

Analysis Tools

A wide variety of analysis tools are available for comprehensive event analysis.

When viewing the analysis tool results, clicking on result will generally take you to the next level of detail for the analysis. For instance, from the Type summary page clicking on a type will display the Normalized Event Summary. Clicking on an even in that list will display the List of Events page featuring that event. Along each progression a new drop-down menu will appear allowing for easy access to either pivot to another analysis tool based on the current view or to return to the previous view.

Additionally most results will have a gear icon next to them. This icon will provide summaries, normally based on time restrictions or a view of the vulnerability summary for the affected host, around that item's result.

For more information, see [Event Analysis Tools](#).

Load Query



The **Load Query** option enables users to load a predefined query and display the current dataset against that query. Click on **Load Query** in the filters list to display a box with all available queries. The query names are displayed in alphabetical order. After clicking on an individual query, the vulnerability view is changed to match the query view for the current dataset.

Event Analysis Filters

For more information, see [Event Analysis Filter Components](#).

Event Analysis Actions

You can use the **Options** drop-down menu to perform the following event analysis actions.

Save Query

You can save the current view as a query for reuse. For more information about queries, see [Queries](#).

Save Asset

Event results can be saved to an asset list for later use. For more information, see [Assets](#).

Save Watchlist

Event results can be saved to a watchlist asset list for later use. For more information, see [Assets](#).

Open Ticket

Tickets are used within Tenable.sc to assist with the assessment and remediation of vulnerabilities and security events. For more information, see [Open a Ticket](#).

View Settings

When available, this setting controls the columns displayed in your view.

Switch to Archived / Switch Archive / Switch to Active

The **Switch to Archived** item is displayed when viewing active event data and when selected will present a dialog to choose the archived event data to display by LCE and date range.



The **Switch Archive** menu item is displayed when viewing archived event data. Selecting this option displays the same menu and selections as above to select a different archive silo for viewing.

The **Switch to Active** menu item is displayed when viewing archived data and when selected, changes the view to active event data for analysis.

Export as CSV

Event results can be exported to a comma-separated file for detailed analysis outside of Tenable.sc by clicking on the Options drop-down menu and then the **Export as CSV** option. When selected, a window opens with an option to choose the columns to be included in the CSV file.

If the record count (rows displayed) of any CSV export is greater than 1,000 records, a note is displayed that prompts for the name of the CSV report to be generated. When complete, the report can be downloaded from the **Report Results** page. For CSV exports of under 1,000 records, the browser's standard **Save As** dialog window is displayed.

Once the appropriate selections are made, click the **Submit** button to create the CSV file or **Cancel** to abort the process.



Event Analysis Tools

A wide variety of analysis tools are available for comprehensive event analysis. Clicking on the drop-down menu indicating the current view (Type Summary by default) displays a list of analysis tools to choose from.

When viewing the analysis tool results, clicking on result will generally take you to the next level of detail for the analysis. For instance, from the Type summary page clicking on a type will display the Normalized Event Summary. Clicking on an even in that list will display the List of Events page featuring that event. Along each progression a new drop-down menu will appear allowing for easy access to either pivot to another analysis tool based on the current view or to return to the previous view.

Additionally most results will have a gear icon next to them. This icon will provide summaries, normally based on time restrictions or a view of the vulnerability summary for the affected host, around that item's result.

Tool	Description
Asset Summary	This tool can be used to see how certain types of activity, remote attackers, or non-compliant events have occurred across different asset groups. Clicking on the Total count for the listed asset displays a Type Summary analysis tool.
Connection Summary	This tool lists connections made between two different hosts by source and destination IP address and the counts of connections between them. Clicking on a host will display the Type Summary analysis tool.
Date Summary	When analyzing large amounts of data, it is often useful to get a quick summary of how the data set manifests itself across several dates. For example, when analyzing a suspected attacker's IP address, creating a filter for that IP address and looking at the type of events is simple enough. However, displaying that same data over the last few days or weeks can paint a much more interesting picture of a potential attacker's activity. Selecting a date will display the Type Summary analysis tool.



Tool	Description
Destination IP Summary	This tool displays events listed by the destination IP address recorded. The table lists the LCE it was discovered on, the IP address, and the count. Clicking on the information icon next to the IP address displays the system information pertaining to the host IP address. Clicking on one of the hosts displays the Type Summary analysis tool.
Detailed Event Summary	This tool displays a summary of the various events based on their full event name and count. Clicking on an event displays the List of Events analysis tool.
Event Trend	This analysis tool displays an event trend area graph with total events over the last 24 hours. Modify the filters for this graph to display the desired event trend view.
IP Summary Class A Summary Class B Summary Class C Summary	Tenable.sc provides the ability to quickly summarize matching IP addresses by single IP address, Class A, Class B, and Class C addresses. The IP Summary tool displays the associated LCE server along with the IP address of the reporting system and about the event count for that system. Clicking on an IP address displays a Host Detail window for that IP address. Clicking the information icon next to the IP address displays information about the NetBIOS Name (if known), DNS Name (if known), MAC address (if known), OS (if known), Score, Repository, Last Scan, Passive Data, Compliance Data, and Vulnerability severity counts. The Assets box displays which asset lists the IP address belongs to. The Useful Links box contains a list of resources that can be queried by IP address. Clicking on one of the Resource links causes the resource to be queried with the current IP address. For example, if the current IP address was a publicly registered address, clicking on the ARIN link causes the ARIN database to be queried for the registration information for that address. If custom resources have been added by an administrative user (via the Manage IP Address Information Links selection under the Customization tab), they will be displayed here.



Tool	Description
	The Sum by Class A, B, and C tools work by displaying matching addresses. Clicking on the number displayed in the Total column will display the Type Summary for that IP address range.
List of Events	This tool displays a line of data for each matching event. The line includes many pieces of information such as time, event name, number of correlated vulnerabilities involved IP addresses, and sensor.
Normalized Event Summary	This tool summarizes a listing of all normalized events and their count for the chosen time period. Normalized events are lower-level events that have been assigned a Tenable name based on LCE scripts parsing of the log records (e.g., Snort-HTTP_Inspect). Clicking on the event name displays the List of Events analysis tool.
Port Summary	A port summary can be invoked. This tool produces a table of the top used ports and combines counts for source and destination ports into one overall count. Clicking on the port will display a Type Summary of events filtered for that port. Note: Port 0 events are host-based events that are not specific to any particular TCP/UDP port.
Protocol Summary	This tool summarizes counts of events based on IP protocols. Clicking on the event total displays a Type Summary view of events filtered by the selected protocol.
Raw Syslog Events	Users can choose to view the original log message or IDS event for full forensic analysis. It is recommended that users attempt some sort of filtering match first before attempting to find their desired event. Users will typically sort their results and drill into the list until they find what they are looking for before attempting to view the raw data.



Tool	Description
Sensor Summary	This tool displays the unique event counts for any query from unique sensor types. When a sensor is clicked on, the Type Summary analysis tool is displayed for events from the selected sensor.
Source IP Summary	This tool displays events listed by the source IP address recorded. The table lists the LCE it was discovered on, the IP address, and the count. Clicking on the information icon next to the IP address displays the system information pertaining to the host IP address. Clicking on one of the hosts displays the Type Summary analysis tool.
Type Summary	This tool displays the matching unique event types and the number of corresponding events for each. The unique event types are based on normalized logs or events such as firewall, system, correlated, network and IDS. These types are high-level types used to describe event types (e.g., login or lce). Clicking on any of the event counts displays the Normalized Event Summary for the type.
User Summary	This tool displays the matching unique event types and the number of corresponding events for each user when user tracking is enabled in LCE. The unique event types are based on normalized logs such as firewall, system, correlated, network, and IDS. Clicking on any of the event counts under the Total column will display the Type Summary analysis tool.



Event Analysis Filter Components

Filters limit the results of the event data displayed and can be added, modified, or reset as desired. For more information, see [Filters](#).

The **Event Analysis** page also supports using a filter bar for filtering. To display the filter bar, click the gear icon Options button and select **Show Filter Bar**.

Note: The filter bar does not display or adjust the time frame filter.

Filter Component	Description
Address	Specifies an IP address, range, or CIDR block to limit the displayed events. For example, entering 198.51.100.64/24 limits any of the web tools to only show event data from that network. Addresses can be entered on separate lines or comma separated.
Asset	Filter the event by the specified asset list. Tip: Use NOT, OR, and AND operators to exclude unwanted assets from the view.
Destination Address	Specifies an IP address or CIDR block to limit the displayed events based on destination. For example, entering 198.51.100.64/24 limits any of the analysis tools to only show event data with destination IPs in that block. Addresses can be comma separated.
Destination Asset	Filter the destination address of the event data by the specified asset list. Tip: Use NOT, OR, and AND operators to exclude unwanted assets from the view.
Destination Port	This filter is in two parts. First the type of filter can be specified to allow matching events with the same ports (=) or different ports (≠). The port filter may specify a single, comma separated list of ports or range of ports (e.g., 8000-8080).
Detailed Event	This is the detailed event name given by the IDS vendor. For example, an event received from a Snort sensor can have a detailed event name of



Filter Component	Description
	DOUBLE DECODING ATTACK, which means that HTTP_INSPECT 119:2:1 fired and was sent to the LCE.
Direction	Filter by event direction of All by default or select Inbound, Outbound, or Internal.
LCEs	Specify the LCE(s) to obtain events from by checking the box next to the choice(s).
Normalized Event	The name given to the event by the LCE after the LCE runs its PRM and TASL scripts against it.
Port	This filter is in two parts. First the type of filter can be specified to allow matching vulnerabilities with the specified ports (=), excluding ports (≠), ports greater than or equal to (≥), or ports less than or equal to (≤). The specified and excluding port filter may specify a single port, comma separated list of ports, or range of ports (e.g., 8000-8080). Note: All host-based vulnerability checks are reported with a port of 0 (zero).
Protocol	Specify the protocol of the event TCP, UDP, or ICMP.
Repositories	Specify the Repositories to obtain events from. The repositories may be searched using the search filter at the top. Multiple repositories may be selected from the list.
Sensor	Filter the events by sensor using the equal (=) or not equal (!=) operators.
Source Address	Specifies an IP address or CIDR block to limit the displayed events based on source. For example, entering 198.51.100.64/24 limits any of the analysis tools to only show event data with source IPs in that block. Addresses can be comma separated.
Source Asset	Filter the source address of the event data by asset list and select an asset list from those available or the NOT operator to exclude asset lists. After each list is added, the AND or OR operator are available to customize the



Filter Component	Description
	combining of asset lists.
Source Port	This filter is in two parts. First the type of filter can be specified to allow matching events with the same ports (=) or different ports (≠). The port filter may specify a single port, comma separated list of ports, or range of ports (e.g., 8000-8080).
Syslog Text	(Raw Syslog Events Analysis Tool) String to search for within the filtered event.
Targeted IDS Events	This filter box selects IDS events that have targeted systems and ports with vulnerabilities likely to be exploited by the detected attack. This is determined by comparing the host's vulnerabilities (CVE, etc.) against those tied to the actual IDS event.
Timeframe	Tip: This filter is always used. By default, it is set for the last 24 hours, based on the time of the page load. An explicit timeframe using the last 24 hours is displayed by default. Specify either an explicit or relative timeframe for the event filter. Choosing explicit allows for selecting dates and times from a calendar and time sliders for the start and end time. Relative timeframes, available from the drop-down box, range using various time periods from the last 15 minutes to the last 12 months and All.
Type	The event type (e.g., error, lce, login, intrusion, etc.) to be filtered on.
User	Specify only events tied to a particular username.

Note: Clicking on **Clear Filters** causes the filters to return to the default settings.



Mobile Analysis

The Mobile analysis page displays lists of vulnerabilities discovered by scanning an ActiveSync, Apple Profile Manager, AirWatch, Good, and/or MobileIron MDM servers.

For information about mobile analysis filtering, see [Mobile Analysis Filter Components](#).

Mobile Analysis Actions

You can use the **Options** drop-down menu to perform the following mobile analysis actions.

Save Query

You can save the current view as a query for reuse. For more information about queries, see [Queries](#).

Export as CSV

You can export mobile results in the current view to a comma-separated file for detailed analysis outside of Tenable.sc.

Note: If the record count (rows displayed) of any CSV export is greater than 1,000 records, a note is displayed that prompts for the name of the CSV report to be generated. When complete, the report can be downloaded from the **Report Results** page. For CSV exports of under 1,000 records, the browser's standard **Save As** dialog window is displayed.

Select the columns of data you want exported, then click **Submit**.



Mobile Analysis Filter Components

For general information about constructing filters, see [Filters](#).

Option	Description
Analysis Tool Filter	
Analysis Tool	This drop-down box is used to choose the analysis tool used by the filter. This is the same as selecting the desired analysis tool from the Analysis > Mobile dialog.
Active Filters	Displays the existing filters and allows the user to selectively remove filters as needed.
Filters	
Identifier	A text based search filter that looks at the Identifier option in the repository.
MDM Type	A drop-down box to select the MDM server type of ActiveSync, Apple Profile Manager, Good, AirWatch, and MobileIron MDM server.
Model	A text based search filter that looks at the Model option in the repository.
Operating System CPE	A text based search filter that looks at the Operating System CPE option in the repository.
Plugin ID	Type the Plugin ID to filter results on.
Plugin Output	Filter results based on a text search of plugin output.
Repositories	Display vulnerabilities from the chosen repositories.
Serial Number	This is a text based search filter that looks at the Serial Number option in the repository.
Severity	Displays vulnerabilities with the selected severity (Info, Low, Medium, High, Critical).
Username	This is a text based search filter that looks at the User option in the



Option	Description
	repository.
Version	This is a text based search filter that looks at the OS Version option in the repository.
Vulnerability Last Observed (Cumulative only)	This filter allows the user to see when the vulnerability was last observed.



Reports

Tenable provides reporting through an assortment of report templates and customizable report formats, including PDF, RTF, 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.sc, 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.sc.

Tip: Tenable provides report templates through the Tenable.sc feed. For a complete index of Tenable-provided report templates, see the [Tenable.sc Report Templates](#) blog.

For more information, see:

- [Manage Reports](#)
- [Manage Report Results](#)
- [CyberScope and DISA Report Attributes](#)
- [Report Images](#)



Manage Reports

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

On the **Reports** page of Tenable.sc, you can manage report definitions and launch reports. For more information, see [Reports](#).

To manage reports:

1. Click **Reporting > Reports**.

The **Reports** page appears.

2. Do any of the following:

- [Filter existing report definitions in the reports table.](#)
- [Create a custom report.](#)
- [Create a template report.](#)
- [Edit a report definition.](#)
- [Edit a report outline.](#)
- [Manage filters for a chapter report.](#)
- [Manage filters for a non-chapter report.](#)
- [View a report definition.](#)
- [Copy a report definition.](#)
- [Export a report definition.](#)
- [Import a report definition.](#)
- [Delete a report definition.](#)
- [Launch a report on demand.](#)
- [Add a report to a scan.](#)



Create a Custom Report

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

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.sc via the user interface.
2. Click **Reporting** > **Reports**.

The **Reports** page appears.

3. Click **Add**.

The **Add Report** page appears.

The **Report Template** page appears.

4. In the **CustomOther** section, click a report tile. For more information, see [Report Templates](#).
5. [Configure the options](#) for the report.

Tenable.sc displays options relevant to the report format you selected.

6. (Optional) [Edit the report outline](#).
7. Click **Submit** to save your report.

Tenable.sc saves your configuration.



Create a Template Report

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

Template reports are formatted reports that can be customized using chapter and target selections. For more information, see [Reports](#).

To create a template report:

1. Log in to Tenable.sc via the user interface.
2. Click **Reporting > Reports**.

The **Reports** page appears.

3. Click **Add**.

The **Add Report** page appears.

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 **TemplateCommon** 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.sc 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.sc creates a report based on the template and displays the **Reports** page. The new report appears as the last entry in reports table.

10. (Optional) Modify report options that are common to both custom and template reports. For 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.



Data Required for Template-Based Reports

Each report template description contains icons that represent which types of data must be available on Tenable.sc to obtain a complete report.

Hover the cursor over the icon to display the label.

Icon	Label	Action Required
	Asset Required	Configure an IPv4/IPv6 repository and store scan results in the repository; see Local Repositories and IPv4/IPv6 Repositories .
	Audit File Required	Upload audit files and add them to your scan policy; see Audit Files and Scan Policies .
	Compliance Data Required	
	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 .
	Active Data Required	Configure a Nessus scanner and run active scans. For more information, see Nessus Scanners and Active Scans .
	Passive Data Required	Configure a Nessus Network Monitor (NNM) scanner; see Nessus Network Monitor Instances .
	Event Data Required	Configure a Log Correlation Engine server; see Log Correlation Engines .



Report Templates

Tenable.sc 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.sc Report Templates](#) blog.

Template	Description
TemplateCommon	
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 Assessments	Reports that aid with identifying vulnerabilities and potential threats.
CustomOther	
PDF	Portable Document Format (PDF); can be viewed universally.
CSV	Comma Separated Values (CSV); can be imported into spreadsheets or databases.
RTF	Rich Text Format (RTF); can be viewed and edited in any text editor.



DISA ARF	(Requires Report Generation configuration) Meets the standards of the Defense Information Systems Agency Assessment Results Format (DISA ARF).
DISA Consolidated ARF	(Requires Report Generation configuration) Meets the standards of the Defense Information Systems Agency Consolidated Assessment Results Format (DISA Consolidated ARF).
DISA ASR	(Requires Report Generation configuration) Meets the standards of the Defense Information Systems Agency Assessment Summary Results (DISA ASR).
CyberScope	(Requires Report Generation configuration) Meets CyberScope reporting standards to support FISMA compliance.



Edit a Report Definition

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

In Tenable.sc, you can edit both custom reports and reports based on templates.

To edit a report definition:

1. Click **Reporting** > **Reports**.

The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

The **Edit Report** page appears.

3. [Modify the report options](#).

Note: Tenable.sc displays options relevant to the report type.

4. (PDF, RTF, and template reports only) [Edit the report outline](#).

5. Click **Submit** to save your changes to the report.



Report Options

In Tenable.sc, you can configure the options described below for both custom and template reports.

Option descriptions below are grouped by the section where they appear in the **Add Report** and **Edit Report** pages. In the option description tables, the **Relevant Reports** column specifies which report types use each option.

Note: Tenable.sc classifies a template-based report as a PDF report. You can configure the same options for that report as you can for a PDF report.

During template report creation, Tenable.sc set these options to default values. You can change these options for a template report only after creation is complete.

- [General Options](#)
- [Report Options](#)
- [Definition Options](#)
- [Display Options](#)
- [Distribution Options](#)

General Options

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.sc displays additional options for the selected time frame.	Any



Option	Description	Relevant Reports
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.	DISA ARF, DISA Consolidated ARF, Cyber-Scope
ASR Content	When creating a report, this drop-down box offers a selection of Benchmark, IAVM, CVE, or Plugin ID to be included.	DISA ASR, 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, Cyber-Scope

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	PDF, RTF



Option	Description	Relevant Reports
	• Tenable 3D — a report with enhanced 3D graphs and a footer logo on the cover page Note: If an administrator configured a Classification Type banner, plain report styles are the only options listed. 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.sc imported the scan results, if you generated the report from scan results • the scan result ID, if you generated the report from scan results	PDF, RTF



Option	Description	Relevant Reports
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, RTF
Include Index	Include an Index with the report.	PDF, RTF
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. The encryption level is 40-bit RC4. When enabled, a password option is displayed for a text entry of a password to use. This password must be used to open the report and view its contents. For more information about this encryption mechanism, please refer to the following URL: https://xm-lgraphics.apache.org/fop/1.0/pdfencryption.html .	PDF

Definition Options



Tenable.sc 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, RTF
Add Template Chapter	A predefined chapter from a Tenable-provided report template. For more information, see Add a Template Chapter to a Report .	PDF, RTF
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, Cyber-Scope; Iterator, Table, and Chart elements in PDF and RTF
Type	The type of data to include in the report.	CSV; Iterator, Table, and Chart elements in PDF and RTF
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	CSV, DISA ARF, DISA Consolidated ARF, DISA ASR, Cyber-Scope; Iterator, Table, and Chart elements in PDF and RTF



Option	Description	Relevant Reports
	◦ Individual Scan—Vulnerabilities identified in a specific scan Note: If you select Individual Scan, Tenable.sc displays the Selected Scan option, which allows you to select a scan to use as the basis of the report: - Click one of the predefined date ranges, or click Custom Range and enter starting and ending days for the range. - Click Fetch Scans to view a list of possible scans within the date range. - Click the scan you want to use in the drop-down box. • If Type is set to Event, valid Source values are: ◦ Active—Currently active events ◦ Archive—Archived events Note: If you select Archive, Tenable.sc displays additional options, allowing you to select the LCE that collected the events and the Silo that stores the archived events. • If Type is set to Mobile, Ticket, or Alert, this option is absent. For DISA ARF, DISA Consolidated ARF, and DISA ASR reports, you do not set the Type option. Valid Source values are limited to Cumulative and Individual Scan, which operate in the same	



Option	Description	Relevant Reports
	way as they do for CSV reports.	
Tool	Select the tool Tenable.sc uses to analyze the data in the report.	CSV; Iterator, Table, and Chart elements in PDF and RTF
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, Cyber-Scope; Iterator, Table, and Chart elements in PDF and RTF
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 .	PDF, RTF

Display Options

These options allow you to specify column format information format. A selection to define the columns and number of results to appear in the report is then available for configuration.

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 and RTF
Sort Column	The column that Tenable.sc uses to sort results in the CSV file. Available columns depend on: the Type you selected in the Definition options	CSV; Iterator, Table, Bar Chart, and Pie Chart elements in PDF and RTF



Option	Description	Relevant Reports
	the Display Columns value you select in the Display options	
Sort Direction	The sort direction for results in the CSV file.	CSV; Iterator, Table, Bar Chart, and Pie Chart elements in PDF and RTF
Display Columns	The columns included in the CSV results file. Available columns depend on Definition options you select.	CSV; Iterator, Table, Bar Chart, and Pie Chart elements in PDF and RTF

Distribution Options

Distribution options specify the actions Tenable.sc takes when a report run completes.

Option	Description	Relevant Reports
Email Users	Allows you to select Tenable.sc users to whom Tenable.sc emails the completed report. The drop-down list includes only users with defined email addresses.	Any
Email Addresses	Allows you to add email addresses where Tenable.sc emails the completed report. You can specify multiple email addresses, separated by commas.	Any
Share	Allows you to select which Tenable.sc users within your organization can view the completed report in Tenable.sc. Use this option if organizational policies prohibit emailing potentially sensitive data.	Any
Publishing Sites	Allows you to select predefined publishing sites where Tenable.sc uploads the completed report. For more information, see Publishing Sites Settings .	Any



Edit a Report Outline

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

In Tenable.sc, the report outline allows you to modify the structure of a PDF, RTF, or template-based report.

The outline consists of the following components:

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.

To edit a report outline:

1. Click **Reporting > Reports**.

The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

The **Edit Report** page appears.

3. In the left navigation bar, click **Definition**.

The report outline appears. The outline is, by default, expanded.

4. In the report outline, you can:

- Expand or collapse elements nested in the outline by clicking **Collapse All** or **Expand All** in the top navigation bar.
- Expand or collapse elements nested in an individual chapter or element by clicking the arrow next to the element.
- [Add a custom chapter](#).
- [Add a template chapter](#).



- [Add or edit a report element.](#)
- [Reorder chapters and elements in a report.](#)
- Delete a report element by clicking the delete icon next to the element.

Note: Tenable.sc does not ask you to confirm this deletion. However, the deletion is not final until you save all changes to the report.

5. Click **Submit** to save your changes to the report.



Add a Custom Chapter to a Report

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

In Tenable.sc, you can add custom chapters to PDF, RTF, or template-based reports.

To add a custom chapter to a report definition:

1. Click **Reporting** > **Reports**.

The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

The **Edit Report** page appears.

3. In the left navigation bar, click **Definition**.

The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).

4. In the bottom navigation bar of the report outline, click **Add Chapter**

Tip: If the report contains multiple chapters or sections, scroll down to locate the bottom navigation bar. It can also be helpful to click **Collapse All** on the top navigation bar to collapse the outline to its highest-level components.

The **Add Chapter** page appears.

5. In the **Name** box, enter a title for the chapter.
6. In the **Location** box, select a relative location for the chapter within the report.
7. In the **Style** box, select a style for the report.
8. Click **Submit**.

Tenable.sc adds the chapter to the report and displays the **Edit Report** page.

9. Click **Submit** to save your changes to the report.



Add a Template Chapter to a Report

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

In Tenable.sc, you can add template chapters to template reports and custom PDF or RTF reports.

To add a template-based chapter to a report definition:

1. Click **Reporting** > **Reports**.

The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

The **Edit Report** page appears.

3. In the left navigation bar, click **Definition**.

The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).

4. In the top navigation bar of the outline, click **Add Template Chapter**.

5. Do one of the following:

- In the **Search Templates** box in the top right corner of the page, search for a specific template by keyword.

Tip: After the initial search, you can limit search results by template category.

- Click a template category icon to view the related templates.

6. Click the report template that contains chapters you want to include in your custom report.

7. (Optional) Modify the default options for the report template:

- a. In the **Chapters** section, select which chapters from the template you want to include in your report. By default, the report includes all chapters from the template.



b. Do one of the following:

- In the **Focus** section, target all systems in the report.

This is the default setting. To return to this setting, click **All Systems** in the **Targets** drop-down box.

- Target specific assets in the report.

i. In the **Targets** drop-down box, click **Assets**.

ii. Select **Assets** and **Repositories**.

- Target specific IP addresses in the report.

i. In the **Targets** drop-down box, click **IP Addresses**.

ii. In the **IP Addresses** box, type the IP address or addresses where you want the report to focus. Use commas to separate multiple addresses.

iii. In the **Repositories** box, select a target repository or repositories.

- Target specific repositories in the report.

i. In the **Targets** drop-down box, click **Repositories**.

ii. In the **Repositories** box, select a target repository or repositories.

c. (Optional) Edit text in the **Description** box.

Note: You cannot modify any information in the **Details** section.

8. Click **Add**.

Tenable.sc adds the template chapter or chapters to your custom report and displays the **Add Report** page again.

9. (Optional) Change the template chapter options.

a. Click the edit icon next to the chapter you added.

b. In the **Name** box, edit the chapter title.



- c. In the **Location** box, change the relative location for the chapter within the report.
 - d. In the **Style** box, select a style for the chapter.
 - e. Click **Submit** to save your changes to the chapter.
10. Click **Submit** to save your changes to the report.



Add or Edit a Report Element

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

You can add or edit elements within chapters or grouping elements in Tenable.sc reports.

To add or edit a report element:

1. Click **Reporting** > **Reports**.

The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

The **Edit Report** page appears.

3. In the left navigation bar, click **Definition**.

The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).

4. Do one of the following:

- Click **Add Element** next to the element where you want to add the element.
- Click the edit icon next to the element you want to change.

Tip: To display **Add Element** or the edit icon, hover the cursor over the element.

5. Configure any of the following types of elements:

- **Grouping**
- **Text**
- **Charts**

6. Click **Submit** to save your changes to the report.



Configure a Grouping Element in a Report

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

Grouping elements in Tenable.screports include:

Type	Description	Relevant Reports
Group	Groups associated elements on the same page.	PDF, RTF
Section	Allows you to organize content within chapters.	PDF, RTF
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, RTF

To configure a grouping element:

1. Click **Reporting > Reports**.

The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

The **Edit Report** page appears.

3. In the left navigation bar, click **Definition**.

The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).

4. Click **Add Element**.

Tip: To display **Add Element**, hover the cursor over the element.



5. Do one of the following:

- Add a group to the report.
 - a. In the **Grouping** section, click the **Group** icon.
 - b. Configure the following options:

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.sc 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 Event, valid Source values are: Active—Currently active events Archive—Archived events Note: If you select Archive, Tenable.sc displays additional options, allowing you to select the LCE that collected the events and the Silo that stores the archived events.
Filters	Specify additional criteria to refine element data. See Manage Filters for a Chapter Report
Iterator Type	Select a grouping method for iteration data: IP Summary—Group vulnerability or event data by the IP addresses of detected hosts. Port Summary—Group vulnerability or event data by the detected ports. Type Summary—Group event data by event type. User Summary—Group event data by user. Vulnerability Summary—Group vulnerability data by individual vulnerability.
Results Displayed	Select the number of results you want to include in the iteration.
Sort Column	Select the column that Tenable.sc uses to sort the iteration data.



Sort Direction	Select the sort direction for the iteration data.
Header Information	Select the columns you want to include in the iteration data. Available columns depend on the settings of the Type and Source options.

6. Click **Submit** to save the element.
7. Click **Submit** to save your changes to the report.



Configure a Text Element in a Report

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

Text elements in Tenable.sc reports include:

Type	Description	Relevant Reports
Matrix	Data in a chart layout.	PDF, RTF
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.sc presents the user with the ability to choose a vulnerability-centric report (a listing of vulnerabilities with all associated hosts).	PDF, RTF
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, RTF
Assurance Report Card	An element based on the results of a selected Assurance Report Card.	PDF, RTF

To configure a text element in a report:

1. Click **Reporting > Reports**.

The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

The **Edit Report** page appears.

3. In the left navigation bar, click **Definition**.

The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).



4. Do one of the following:

- Click **Add Element** to add an element.
- Click the edit icon next to the element to edit an existing element.

Tip: To display **Add Element** and the edit icon, hover the cursor over the element.

5. Do one of the following:

- [Add a matrix to the report.](#)
- [Add a table to the report.](#)
- Add a paragraph to the report.
 - a. In the **Text** section, click the **Paragraph** icon.
 - b. Configure the following options:

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

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

A matrix element is a type of text element you can insert into a Tenable.sc report definition. For more information on text elements, see [Configure a Text Element in a Report](#).

To configure a matrix element in a report:

1. Click **Reporting** > **Reports**.

The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

The **Edit Report** page appears.

3. In the left navigation bar, click **Definition**.

The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).

4. Do one of the following:

- Add a new element.
 - a. Click **Add Element**.
 - b. In the **Text** section, click the **Matrix** icon.
- Click the edit icon next to the element you want to change.

Tip: To display **Add Element** and the edit icon next to an element, hover the cursor over the element.

5. Configure the **General** options:

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.sc displays the empty matrix for configuration.

8. Do one of the following:
 - Edit a row or column header.
 - a. Click the header for the row or column you want to edit.
 - b. Next to the header label, click the  menu.

The actions menu appears.
 - c. Click **Edit Header**.
 - d. In the **Label** box, type a new header.
 - e. Click **Submit**.
 - Add a matrix component.
 - a. Click the matrix cell where you want to add the component.
 - b. In the **Data Type** drop-down box, select the type of data for the component.
 - c. In the **Type** drop-down box, select the type of calculation you want the component to perform.
 - d. In the **Source** drop-down box, select a data source.
 - e. (Optional) In the **Filter** box, add or edit a filter using the same steps you would to add a filter to a report element; see [Manage Filter Components for a Single Element](#).
 - f. In the **Rules** section, click **Add Rule** to add a rule.



-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.sc inserts the copied column to the right of the original column

For rows, Tenable.sc inserts the copied row under the original row.

- Delete a row or column.

a. Click the header for the row or column you want to delete.

b. Next to the header label, click the  menu.

The actions menu appears.

c. Click **Delete Cells**.

9. Click **Submit** to save your changes to the element.

10. Click **Submit** to save your changes to the report.

Example

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

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

A table element is a type of text element you can insert into a Tenable.sc report definition. For more information on text elements, see [Configure a Text Element in a Report](#).

To configure a table element in a report:

1. Click **Reporting > Reports**.

The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

The **Edit Report** page appears.

3. In the left navigation bar, click **Definition**.

The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).

4. Do one of the following:

- Add a new element.
 - a. Click **Add Element**.
 - b. In the **Text** section, click the **Table** icon.
- Click the edit icon next to the element you want to change.

Tip: To display **Add Element** and the edit icon next to an element, hover the cursor over the element.

5. Configure the **General** options:

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]

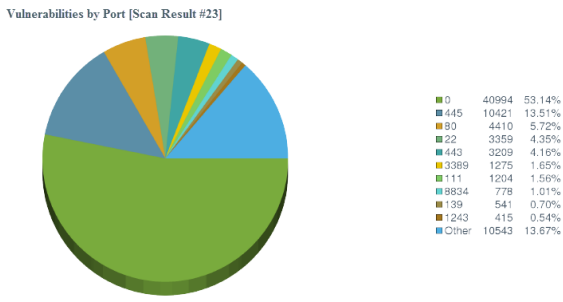
Asset	Score	Total	Med.	High	Crit.
All Defined Assets	13593	1423	541	777	105
Linux Hosts	4189	476	193	257	26
Linux Kernel 2.6	4092	453	174	253	26
CentOS	3625	386	115	252	19
Linux Kernel 64-Bit	1294	141	68	61	12
Ubuntu Linux	380	48	40	2	6
Debian Linux	74	10	8	1	1
Linux Kernel 3.1	9	3	3	0	0
Linux Kernel 3.2	6	2	2	0	0
Linux Kernel 3.3	6	2	2	0	0



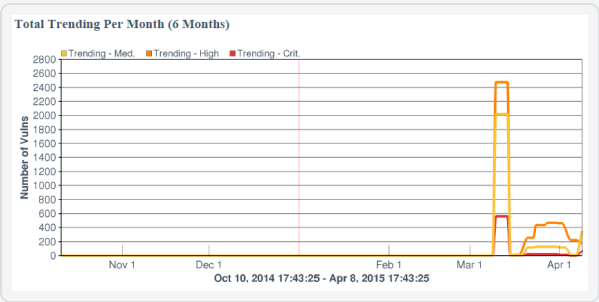
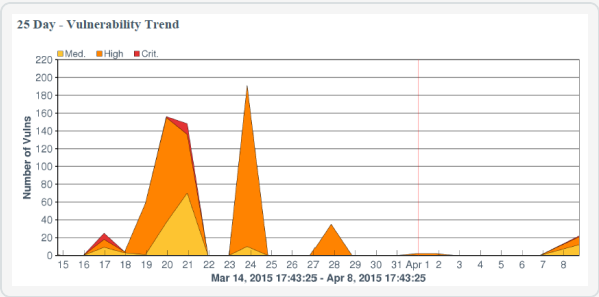
Configure a Charts Element in a Report

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

Charts elements in Tenable.sc reports include:

Option	Description	Relevant Reports																																												
Bar Chart	Click to add a bar chart element to the report. Asset Summary by Severity [Scan Result #14] <table><thead><tr><th>Asset</th><th>Med.</th><th>High</th><th>Crit.</th></tr></thead><tbody><tr><td>All Defined Assets</td><td>550</td><td>800</td><td>150</td></tr><tr><td>Linux Hosts</td><td>200</td><td>280</td><td>50</td></tr><tr><td>Linux Kernel 2.6</td><td>200</td><td>280</td><td>50</td></tr><tr><td>CentOS</td><td>150</td><td>280</td><td>50</td></tr><tr><td>Linux Kernel 6.8-88</td><td>100</td><td>80</td><td>50</td></tr><tr><td>Ubuntu Linux</td><td>50</td><td>50</td><td>50</td></tr><tr><td>Debian Linux</td><td>50</td><td>50</td><td>50</td></tr><tr><td>Linux Kernel 3.2</td><td>50</td><td>50</td><td>50</td></tr><tr><td>Linux Kernel 3.2</td><td>50</td><td>50</td><td>50</td></tr><tr><td>Linux Kernel 3.2</td><td>50</td><td>50</td><td>50</td></tr></tbody></table>	Asset	Med.	High	Crit.	All Defined Assets	550	800	150	Linux Hosts	200	280	50	Linux Kernel 2.6	200	280	50	CentOS	150	280	50	Linux Kernel 6.8-88	100	80	50	Ubuntu Linux	50	50	50	Debian Linux	50	50	50	Linux Kernel 3.2	50	50	50	Linux Kernel 3.2	50	50	50	Linux Kernel 3.2	50	50	50	PDF, RTF
Asset	Med.	High	Crit.																																											
All Defined Assets	550	800	150																																											
Linux Hosts	200	280	50																																											
Linux Kernel 2.6	200	280	50																																											
CentOS	150	280	50																																											
Linux Kernel 6.8-88	100	80	50																																											
Ubuntu Linux	50	50	50																																											
Debian Linux	50	50	50																																											
Linux Kernel 3.2	50	50	50																																											
Linux Kernel 3.2	50	50	50																																											
Linux Kernel 3.2	50	50	50																																											
Pie Chart	Click to add a pie chart element to the report. Vulnerabilities by Port [Scan Result #23] <table><thead><tr><th>Port</th><th>Count</th><th>Percentage</th></tr></thead><tbody><tr><td>0</td><td>40994</td><td>53.14%</td></tr><tr><td>445</td><td>10421</td><td>13.51%</td></tr><tr><td>80</td><td>4410</td><td>5.72%</td></tr><tr><td>22</td><td>3359</td><td>4.35%</td></tr><tr><td>443</td><td>3209</td><td>4.16%</td></tr><tr><td>3389</td><td>1275</td><td>1.65%</td></tr><tr><td>111</td><td>1204</td><td>1.56%</td></tr><tr><td>8834</td><td>778</td><td>1.01%</td></tr><tr><td>139</td><td>541</td><td>0.70%</td></tr><tr><td>1243</td><td>415</td><td>0.54%</td></tr><tr><td>Other</td><td>10543</td><td>13.67%</td></tr></tbody></table>	Port	Count	Percentage	0	40994	53.14%	445	10421	13.51%	80	4410	5.72%	22	3359	4.35%	443	3209	4.16%	3389	1275	1.65%	111	1204	1.56%	8834	778	1.01%	139	541	0.70%	1243	415	0.54%	Other	10543	13.67%	PDF, RTF								
Port	Count	Percentage																																												
0	40994	53.14%																																												
445	10421	13.51%																																												
80	4410	5.72%																																												
22	3359	4.35%																																												
443	3209	4.16%																																												
3389	1275	1.65%																																												
111	1204	1.56%																																												
8834	778	1.01%																																												
139	541	0.70%																																												
1243	415	0.54%																																												
Other	10543	13.67%																																												
Line Chart	Click to add a line chart element to the report.	PDF, RTF																																												



Option	Description	Relevant Reports
	 Line charts are defined by time (x-axis) and series data (y-axis). When selecting the time, available options include Relative time and Absolute time. One or more series data elements can be chosen and displayed as discrete lines for easy comparison.	
Area Chart	Click to add an area chart element to the report.  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.	PDF, RTF

To configure a chart element in a report:

1. Click **Reporting > Reports**.

The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.



The **Edit Report** page appears.

3. In the left navigation bar, click **Definition**.

The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).

4. Do one of the following:

- Add a chart element
 - a. Click **Add Element** to add an element.
 - b. In the **Charts** section, click the icon for the type of chart you want to add.
- Click the edit icon next to an existing chart element.

Tip: To display **Add Element** and the edit icon, hover the cursor over the element.

5. For all charts, configure the **General** options:

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

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

In Tenable.sc, you can reorder chapters and elements in a PDF, CSV, or template-based report.

To reorder report chapters and elements:

1. Click **Reporting** > **Reports**.

The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

The **Edit Report** page appears.

3. In the left navigation bar, click **Definition**.

The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).

4. Do one of the following:

- In the report outline, click the report element, then drag and drop it to its new location.
- Click the edit icon for the component, and select a new location in the **Location** drop-down box.

5. Click **Submit** to save your changes to the report.



Manage Filters for a Chapter Report

In Tenable.sc, PDF, RTF, and template-based reports use a chapter structure, so you can specify different filters for individual chapter elements of those reports.

You can manage filters for a single element or for multiple elements at the same time. For more information, see:

- [Manage Filter Components for a Single Element](#)
- [Manage Filter Components for Multiple Elements](#)



Manage Filter Components for a Single Element

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

Tip: You can build filters using one or more *filter components* with defined *filter component criteria*. Filter components are types of data (e.g., **CVE ID** or **Severity**). After you select a filter component, you specify the filter component criteria (e.g., a specific CVE ID or a specific severity level).

To manage filter components for a single element in a chapter report in Tenable.sc:

1. Click **Reporting > Reports**.

The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

The **Edit Report** page appears.

3. In the left navigation bar, click **Definition**.

The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).

4. Click the edit icon next to the element you want to edit.

Tip: To display icons next to a element, hover the cursor over the element.

5. Do one of the following:

- Add a filter component.

Use these steps to add one or more filter components to a single element. For information about the filter components available for vulnerability analysis data or event analysis data, see [Vulnerability Analysis Filter Components](#) or [Event Analysis Filter Components](#).

- a. In the **Data** section, click **Add Filter**.
- b. Select a filter component from the drop-down box.
- c. Set the filter component criteria, as prompted.



Depending on the filter component you selected, Tenable.sc prompts you to type the value you want to filter for or to select from valid values and operators.

Note: If Tenable.sc does not prompt you to specify an operator, the unstated operator is equivalent to **is equal to** or **is set to**.

- d. Click the check mark next to the filter component to stop editing it.

Note: The new filter component is not saved until you click **Submit**.

- Edit a filter component.

- a. In the **Data** section, click the edit icon next to the filter component.
- b. Edit the filter component criteria.
- c. Click the check mark next to the filter component to stop editing it.

Note: Your changes to the filter are not saved until you click **Submit**.

- Delete a filter component.

In the **Data** section, click the delete icon next to the filter component.

Note: Tenable.sc does not prompt you to confirm the deletion. However, the deletion is not final until you click **Submit** to save your changes.

6. Click **Submit**.



Manage Filter Components for Multiple Elements

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

When managing filter components for a chapter report in Tenable.sc, you can search the report for elements that use certain filter components, then update the filter component criteria for all matching elements in that report at the same time.

Tip: You can build filters using one or more *filter components* with defined *filter component criteria*. Filter components are types of data (e.g., **CVE ID** or **Severity**). After you select a filter component, you specify the filter component criteria (e.g., a specific CVE ID or a specific severity level).

You can use the following filter components to search and update: **Address**, **Audit File**, **Asset**, **CVE ID**, **DNS Name**, **IAVM ID**, **Repositories**, **Scan Policy**, and **Severity**.

For example, if you search a report definition for all elements where the **Severity** filter component is set to **Info**, you can update the **Severity** filter component to **Medium** for all elements, and add an **Audit File** filter component to the elements at the same time.

To manage filter components for multiple elements in a chapter report:

1. Click **Reporting > Reports**.

The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

The **Edit Report** page appears.

3. In the left navigation bar, click **Definition**.

The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).

4. In the top navigation bar of the outline, click **Find/Update Filters**.

To search for specific elements in the report:

1. In the **Search Filters** section, click **Add Search Filter**.
2. Select a filter component from the drop-down box.



3. Select an operator from the drop-down box.
 - a. If you selected **is equal to** or **contains** as operator, type filter component criteria or select a value from the list of valid filter component criteria, as appropriate to the filter component you selected.
4. Click the check mark at the end of the filter box.

Tenable.sc searches the report outline for elements that match your search criteria and displays the results in the **Matching Filters** box.

To specify the filter updates you want to make:

1. In the **Update Actions** section, click **Add Search Filter**.
2. Select a filter component from the drop-down box.
3. Select an operator from the drop-down box.
4. Type filter component criteria or select a value from the list of valid filter values, as appropriate to the filter component and operator you selected.
5. Click the check mark at the end of the filter box.

To review and update the filter updates:

1. In the **Matching Filters** box, review the list to verify that you want to apply the update to all the listed elements.

Tip: If you do not want to apply the current update to all the listed elements, it may be more appropriate to manage filter components by individual element. For more information, see [Manage Filter Components for a Single Element](#).

2. Click **Update Filters**.

Tenable.sc applies the updates to the matching elements and returns you to the report outline.

3. Click **Submit** to save your changes to the report.



Manage Filter Components for a Non-Chapter Report

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

In Tenable.sc, CSV, DISA ARF, DISA ASR, and Cyberscope reports do not use a chapter structure, so you can create a set of filter components that apply to every element of the report.

Tip: You can build filters using one or more *filter components* with defined *filter component criteria*. Filter components are types of data (e.g., **CVE ID** or **Severity**). After you select a filter component, you specify the filter component criteria (e.g., a specific CVE ID or a specific severity level).

To manage filter components for a non-chapter report:

1. Click **Reporting > Reports**.

The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

The **Edit Report** page appears.

3. Do one of the following:

- Add a filter component.

Use these steps to add one or more filter components to a single element. For information about the filter components available for vulnerability analysis data or event analysis data, see [Vulnerability Analysis Filter Components](#) or [Event Analysis Filter Components](#).

- a. In the **Definition** section, click **Add Filter**.
- b. Select a filter component from the drop-down box.
- c. Set the filter component criteria, as prompted.

Depending on the filter component you selected, Tenable.sc prompts you to type the value you want to filter for or to select from valid values and operators.



- d. Click the check mark next to the filter component to stop editing it.

Note: The new filter component is not saved until you click **Submit**.

- Edit a filter component.
 - a. In the **Definition** section, click the edit icon next to the filter component.
 - b. Edit the filter criteria.
 - c. Click the check mark next to the filter component to stop editing it.

Note: Your changes to the filter component are not saved until you click **Submit**.

- Delete a filter component.

In the **Definition** section, click the delete icon next to the filter component.

Note: Tenable.sc does not prompt you to confirm the deletion. However, the deletion is not final until you click **Submit** to save your changes.

4. Click **Submit** to save your changes.



View a Report Definition

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

To view a report definition:

1. Click **Reporting** > **Reports**.

The **Reports** page appears.

2. In the row for the report definition you want to view, click the  menu.

The actions menu appears.

3. Click **View**.

Tenable.sc displays a read-only version of the report definition.

Note: If you want to edit or delete the report definition from this page, see [Edit a Report Definition](#) or [Delete a Report Definition](#).



Copy a Report Definition

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

You can share a copy of a report definition with other users in your organization in Tenable.sc. This feature is useful for maintaining consistency throughout your organization.

After you share the copy, the other users own their local copy and can edit or delete as with any report they create themselves. Later changes you make to the original do not synchronize automatically to the copy.

To copy a report definition:

1. Click **Reporting > Reports**.

The **Reports** page appears.

2. In the row for the report you want to copy, click the  menu.

The actions menu appears.

3. Click **Copy**.

The **Copy Report** page appears.

4. In the **Group** box, select the group you want to grant access to a copy of the report.
5. Specify the user(s) that you want to grant access to a copy of the report.
6. Click **Copy**.

Tenable.sc copies the report definition to the other accounts you specified. The copy appears, named **Copy of DefinitionName**.



Export a Report Definition

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

In Tenable.sc, you can export a report definition as an `.xml` file. This feature is useful for organizations running multiple Tenable.sc deployments to provide consistent reports without duplicating the work needed to create definition templates.

To export a report definition:

1. Click **Reporting** > **Reports**.

The **Reports** page appears.

2. In the row for the definition you want to export, click the  menu.

The actions menu appears.

3. Click **Export**.



4. 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.sc downloads the report definition to your computer.



Import a Report Definition

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

In Tenable.sc, you can only import XML files in the same format used to [export report definitions](#). This feature is useful for organizations running multiple Tenable.sc deployments to provide consistent reports without duplicating the work needed to create definition templates.

To import a report definition:

1. Copy the report definition file to your local computer.
2. Click **Reporting > Reports**.
The **Reports** page appears.
3. In the top right corner of the page, click **Options**.
4. Click **Import Report**.
5. In the **Name** box, type a name for the report.
6. Click **Choose File** next to the **Report Definition** box.
7. Browse to the local copy of the report definition XML file.
8. Click **Import**.

Tenable.sc imports the report definition.

9. (Optional) [Edit the report definition](#) as desired.



Delete a Report Definition

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

To delete a report definition:

1. Click **Reporting > Reports**.

The **Reports** page appears.

2. In the row for the report you want to delete, click the  menu.

The actions menu appears.

3. Click **Delete**.
4. Click **Delete** to confirm the deletion.

Tenable.sc deletes the report definition.

Note: Tenable.sc retains any report results associated with the deleted definition. You must manually [delete results associated with the report](#).



Launch a Report on Demand

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

To launch a report on demand:

1. Click **Reporting > Reports**.

The **Reports** page appears.

2. Click the gray triangle icon next to the report you want to launch.

Tenable.sc starts the report.

3. (Optional) Monitor the status of the report in the **Report Results** page.

To view this page, do one of the following:

- Click **View Report Results** in the launch notification message.
- Click **Reporting > Report Results** in the top navigation bar.

Note: In the **Report Results** page, you can also [stop the currently running report](#).



Add a Report to a Scan

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

After you create one or more on demand reports, you can add them to active scan, agent scan, or agent synchronization job configurations.

To add a preconfigured report to an active scan, agent scan, or agent synchronization job:

1. Do one of the following:
 - Begin configuring an active scan, as described in [Add an Active Scan](#).
 - Begin configuring an agent scan, as described in [Add an Agent Scan](#).
 - Begin configuring an agent synchronization job, as described in [Add an Agent Synchronization Job](#).
2. In the **Post Scan** section, click **Add Report**.

The page displays available on demand reports.
3. Select the report you want to add.
4. (Optional) If you want the report to include cumulative data in Tenable.sc, enable the **Create report using cumulative data** option.

If you disable this option, the report includes data only from the configured scan.
5. Click the checkmark icon to save the report.
6. (Optional) If you want to add multiple reports, repeat steps 2-5 for each additional report.
7. Click **Submit**.

Tenable.sc saves your configuration.



Manage Report Results

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

On the **Report Results** page of Tenable.sc, you can manage both currently running reports and completed report results. Completed report results include successful and failed report runs, so you can access and distribute a successful report result or troubleshoot a report failure. For more information, see [Reports](#).

To manage report results:

1. Click **Reporting > Report Results**.

The **Report Results** page appears.

2. Do any of the following:

- [Filter existing report results in the report results table.](#)
- [Stop a currently running report.](#)
- [Download a successful report result to your computer.](#)
- [View a successful report result.](#)
- [Publish a successful result.](#)
- [Email a copy of a successful result to specified users.](#)
- [Share a copy of a successful result with other Tenable.sc user accounts.](#)
- [View error conditions for a failed report.](#)
- [Delete a report result.](#)



Stop a Running Report

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

If you want to stop a report that is currently running:

1. Click **Reporting** > **Report Results**.

The **Report Results** page appears.

2. Click the gray square icon next to the report you want to stop.

Tenable.sc stops the report run.

Note: You cannot restart a stopped report run. You can only [launch the report](#) again.



Download a Report Result

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

To download a successful report result to your computer:

1. Click **Reporting > Report Results**.

The **Report Results** page appears.

2. Do one of the following:

- In the Results table, click the name of the report.
- Click the download icon next to the report result in the results table.
- Click the  menu next to the report result.

The actions menu appears.

- a. Click **Download**.



View a Report Result

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

To view a successful report result:

1. Click **Reporting > Report Results**.

The **Report Results** page appears.

2. In the row for the report result you want to view, click the  menu.

The actions menu appears.

3. Click **View**.

The report appears.

4. (Optional) To download the report result to your computer, click **Download**.

The report result downloads.

5. (Optional) To delete the report result, click **Delete**.

Tenable.sc deletes the report result.



Publish a Report Result

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

To publish a successful report result:

1. Click **Reporting > Report Results**.

The **Report Results** page appears.

2. In the row for the report result you want to publish, click the  menu.

The actions menu appears.

3. Click **Publish**.

The **Publish Report Results** window appears.

4. Search for and select a publishing site.

5. Click **Publish**.

Tenable.sc publishes the report result.



Email a Report Result

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

To email a copy of a successful report result to specific users:

1. Click **Reporting** > **Report Results**.

The **Report Results** page appears.

2. In the row for the report result you want to email, click the  menu.

The actions menu appears.

3. Click **Email**.

4. Do one of the following:

- Use the **Group** and **User** boxes to select the Tenable.sc user or users you want to receive the report result.
- Type the email address of recipients who are not Tenable.sc users.

5. Click **Submit**.

Tenable.sc sends the report result.



Copy a Report Result

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

To share a copy of a successful report result with other Tenable.sc user accounts:

1. Click **Reporting > Report Results**.

The **Report Results** page appears.

2. In the row for the report result you want to copy, click the  menu.

The actions menu appears.

3. Click **Copy**.
4. In the **Group** box, select the group you want to grant access to a copy of the report result.
5. Specify a user or users that you want to grant access to a copy of the report result.
6. Click **Copy**.

Tenable.sc copies the report result to the other accounts you specified. The copy appears, named **Copy of ResultName**.



View Errors for a Failed Report

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

To view error conditions for a failed report:

1. Click **Reporting** > **Report Results**.

The **Report Results** page appears.

2. Click the name of the failed result in the results table.

The **View Report Results** page appears.

3. Review the **Error Details** section.



Delete a Report Result

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

To delete a report result:

1. Click **Reporting > Report Results**.

The **Report Results** page appears.

2. In the row for the result you want to delete, click the  menu.

The actions menu appears.

3. Click **Delete**.

A confirmation window appears.

4. Click **Delete** to confirm the deletion.

Tenable.sc 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).
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 (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.



Option	Description
Location	
Tip: Tenable recommends leaving all options blank except the Street Address. The Street Address specifies the COAMS geolocation area.	



Report Images

In Tenable.sc, the **Report Images** interface allows a user with permissions to view details, add, edit, or delete PDF report images. From this interface, you can manage two types of images: logos and watermarks. Logos appear at the bottom of each page, while watermarks appear prominently across the center of the report page.

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.



Assurance Report Cards

Assurance Report Cards (ARCs) provide an overview of the security posture of your network. These configurable reports provide quick visible feedback using a pass/fail methodology for each policy statement in the ARC.

Organizational users with appropriate permissions can add a template-based ARC using Tenable-provided templates or you can add a custom ARC. For more information about Tenable-provided ARC templates, see the [Assurance Report Cards](#) blog. For more information about user permissions, see [User Roles](#).

- [Add a Template-Based Assurance Report Card](#)
- [Add a Custom Assurance Report Card](#)
- [Assurance Report Card Options](#)
- [Edit an Assurance Report Card](#)
- [View Your Assurance Report Cards](#)
- [View Details for an Assurance Report Card](#)
- [Share or Revoke Access to an Assurance Report Card](#)
- [Export an Assurance Report Card](#)
- [Copy an Assurance Report Card](#)
- [Delete an Assurance Report Card](#)



Add a Template-Based Assurance Report Card

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

You can use a Tenable-provided template to add an Assurance Report Card (ARC). For more information about Tenable-provided ARC templates, see the [Assurance Report Cards](#) blog. To create a custom ARC, see [Add a Custom Assurance Report Card](#).

For more information, see [Assurance Report Cards](#).

To add a template-based Assurance Report Card:

1. Log in to Tenable.sc via the user interface.
2. Click **Dashboard > Assurance Report Cards**.

The **Assurance Report Cards** page appears.

3. Click **Add**.

The **Add Assurance Report Cards** page appears.

The **Assurance Report Card Templates** page appears.

4. Click a template category tile.

The **Select Assurance Report Card Template** page appears.

The list of templates for the selected category appears.

5. Click a template.

The **Add Assurance Report Card Template** page updates to reflect the template you selected.

6. Modify the ARC template. For more information, see [Assurance Report Card Options](#).
 - To edit the ARC name, click ARC template title.
 - To edit the ARC description, click the **Description** box.
 - To edit the required assets, click an item in the **Required Assets** section.



- To restrict the target data displayed in the ARC, click the **Targets** drop-down box.
- To set how often the ARC polls data sources to obtain updates, click **Schedule**.

7. Click **Add**.

Tenable.sc saves your configuration.



Add a Custom Assurance Report Card

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

You can create a fully customized Assurance Report Card (ARC). To add an ARC from a Tenable-provided template, see [Add a Template-Based Assurance Report Card](#).

For more information, see [Assurance Report Cards](#).

To add a custom Assurance Report Card:

1. Log in to Tenable.sc via the user interface.
2. Click **Dashboard** > **Assurance Report Cards**.

The **Assurance Report Cards** page appears.

3. In the **Options** dropdown box, click **Advanced Add**.

The **Advanced Add Assurance Report Cards** page appears.

4. Configure the ARC options. For more information, see [Assurance Report Card Options](#).
5. Click **Submit**.

Tenable.sc saves your configuration.



View Your Assurance Report Cards

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

You can view a summary that displays each Assurance Report Card (ARC), the overall status of the ARC, and the status of each policy statement in each ARC. To view details for an ARC, see [View Details for an Assurance Report Card](#).

For more information, see [Assurance Report Cards](#).

Tip: To change the position of an ARC in the list, click the icon next to the ARC and drag it to a new position.

Before you begin:

- Add an ARC, as described in [Add a Template-Based Assurance Report Card](#) or [Add a Custom Assurance Report Card](#).

To view a summary of your Assurance Report Cards:

1. Log in to Tenable.sc via the user interface.
2. Click **Dashboard** > **Assurance Report Cards**.

The **Assurance Report Cards** page appears.

3. Click the row for the ARC.

The ARC expands to display each policy statement in the ARC.

4. View the status of each ARC and its policy statements.
 - A green icon (✓) next to an ARC indicates all policy statement in the ARC passed.
 - A red icon (✗) next to an ARC indicates one or more policy statements in the ARC failed.
 - A green check mark (✓) next to a policy statement indicates the policy statement passed.
 - A red x (✗) next to a policy statement indicates the policy statement failed.

What to do next:



- (Optional) Click a policy statement to view vulnerability analysis for the policy statement data.
For more information, see [Vulnerability Analysis](#).



View Details for an Assurance Report Card

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

For more information, see [Assurance Report Cards](#).

Before you begin:

- Add an Assurance Report Card (ARC), as described in [Add a Template-Based Assurance Report Card](#) or [Add a Custom Assurance Report Card](#).

To view details for an Assurance Report Card:

1. Log in to Tenable.sc via the user interface.
2. Click **Dashboard > Assurance Report Cards**.

The **Assurance Report Cards** page appears.

3. In the **Options** drop-down menu, click **Manage ARCs**.

The **Manage Assurance Report Cards** page appears.

4. In the row for the ARC for which you want to view details, click the  menu.

The actions menu appears.

5. Click **View**.

The **View Assurance Report Card** page appears. For more information, see [Assurance Report Card Options](#).

Section	Action
Options drop-down box	• To edit the ARC, click Edit. • To delete the ARC, click Delete.
General	View general information about the ARC. • Name — The ARC name. • Description — The ARC description.



Section	Action
	• Schedule – TheARC schedule. • Created – The date the ARC was created. • Last Modified – The date the ARC was last modified. • Owner – The user who created or owns the ARC. • Group – The group associated with the Owner. • ID – The unique identifier for the ARC.
Policy Statements	View the policy statements in the ARC.
Focus	View the targets configured for the ARC.



Edit an Assurance Report Card

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

For more information, see [Assurance Report Cards](#).

Before you begin:

- Add an Assurance Report Card (ARC), as described in [Add a Template-Based Assurance Report Card](#) or [Add a Custom Assurance Report Card](#).

To edit an Assurance Report Card:

1. Log in to Tenable.sc via the user interface.
2. Click **Dashboard** > **Assurance Report Cards**.

The **Assurance Report Cards** page appears.

3. In the **Options** drop-down menu, click **Manage ARCs**.

The **Manage Assurance Report Cards** page appears.

4. In the row for the ARC you want to edit, click the  menu.

The actions menu appears.

5. Click **Edit**.

The **Edit Report Card** page appears.

6. Modify the ARC options. For more information, see [Assurance Report Card Options](#).

7. Click **Submit**.

Tenable.sc saves your configuration.



Share or Revoke Access to an Assurance Report Card

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

You can share access to an Assurance Report Card (ARC) to give users in a group the ability to view the ARC. The user's role and custom permissions determine if they can drill down into other pages with more information. For more information, see [Assurance Report Cards](#).

Before you begin:

- Add an ARC, as described in [Add a Template-Based Assurance Report Card](#) or [Add a Custom Assurance Report Card](#).

To share or revoke access to an Assurance Report Card:

1. Log in to Tenable.sc via the user interface.
2. Click **Dashboard > Assurance Report Cards**.

The **Assurance Report Cards** page appears.

3. In the **Options** drop-down menu, click **Manage ARCs**.

The **Manage Assurance Report Cards** page appears.

4. In the row for the ARC for which you want to share or revoke access, click the  menu.

The actions menu appears.

5. Click **Share**.

The **Share Assurance Report Card** page appears.

6. In the box, search for and select the groups for which you want to share or revoke access.
7. Click **Submit**.

Tenable.sc saves your configuration.



Export an Assurance Report Card

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

You can export an Assurance Report Card (ARC) to share with other users in your organization. For more information, see [Assurance Report Cards](#).

Before you begin:

- Add an ARC, as described in [Add a Template-Based Assurance Report Card](#) or [Add a Custom Assurance Report Card](#).

To export an Assurance Report Card:

1. Log in to Tenable.sc via the user interface.
2. Click **Dashboard** > **Assurance Report Cards**.

The **Assurance Report Cards** page appears.

3. In the **Options** drop-down menu, click **Manage ARCs**.

The **Manage Assurance Report Cards** page appears.

4. In the row for the ARC you want to export, click the  menu.

The actions menu appears.

5. Click **Export**.

The export options appear.



6. Click the export option you want to use:

Option	Description
Keep All References	Export the ARC with object references intact. Users who meet the following requirements can use an imported ARC with intact object references: • The user must be in the same organization as the user who exported the ARC. • The user must have access to all relevant objects in the ARC.
Remove All References	Export the ARC with object references removed, altering the definitions of the components. Any user can use an imported ARC with object references removed.
Replace With Placeholders	Export the ARC 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 ARC with placeholder names.
Template	Export the ARC as a template.

Tenable.sc exports the ARC as an `.xml` file.



Copy an Assurance Report Card

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

For more information, see [Assurance Report Cards](#).

Before you begin:

- Add an Assurance Report Card (ARC), as described in [Add a Template-Based Assurance Report Card](#) or [Add a Custom Assurance Report Card](#).

To copy an Assurance Report Card:

1. Log in to Tenable.sc via the user interface.
2. Click **Dashboard > Assurance Report Cards**.

The **Assurance Report Cards** page appears.

3. In the **Options** drop-down menu, click **Manage ARCs**.

The **Manage Assurance Report Cards** page appears.

4. In the row for the ARC you want to copy, click the  menu.

The actions menu appears.

5. Click **Copy**.

Tenable.sc copies the ARC. The copy appears, named **Copy of ARCName**.



Delete an Assurance Report Card

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

For more information, see [Assurance Report Cards](#).

To delete an Assurance Report Card (ARC):

1. Log in to Tenable.sc via the user interface.
2. Click **Dashboard** > **Assurance Report Cards**.

The **Assurance Report Cards** page appears.

3. In the **Options** drop-down menu, click **Manage ARCs**.

The **Manage Assurance Report Cards** page appears.

4. In the row for the ARC you want to delete, click the  menu.

The actions menu appears.

5. Click **Delete**.

A confirmation window appears.

6. Click **Delete**.

Tenable.sc deletes the ARC.



Assurance Report Card Options

You can configure the following options for Assurance Report Cards (ARCs). For more information, see [Assurance Report Cards](#).

- [Assurance Report Card Options](#)
- [Policy Statement Options](#)

Assurance Report Card Options

Option	Description
General	
Name	The name of the ARC.
Description	(Optional) A description for the ARC.
Schedule	Specifies how often the ARC polls data sources to obtain updates. • Daily (default) – The ARC polls data sources every 1-20 days at the specified time. • Weekly – The ARC polls data sources every 1-20 weeks at the specified time and day of the week. • Monthly – The ARC polls data sources every 1-20 months at the specified time and day of the month. For example, <i>Every 2 months on the fourth Thursday at 15:00 -4:00</i> indicates the ARC will poll data sources to obtain updates every two months, on the fourth Thursday of the month, at 15:00 in the America/New York timezone.
Policy Statements	
Add Policy Statement	Click to add a custom policy statement to the ARC. For more information, see Policy Statement Options .
Focus	
Targets	Specifies the target hosts for the ARC to analyze:



Option	Description
	• All Systems – Targets all available hosts. • Assets – Targets the specified assets. For more information, see Assets. Tip: Use NOT, OR, and AND operators to exclude unwanted assets from the view. • IPs – Targets the specified IP addresses. You can specify single addresses, IP addresses in CIDR notation, and IP ranges. • Repositories – Targets the specified repositories. For more information, see Repositories. If you want to match the specified assets or IP addresses against one or more repositories, select the repositories you want to match against. Note: If an IP address you specified appears in two or more repositories you selected, the duplicated IP address negatively skews the ARC results.

Policy Statement Options

Option	Description
Basic	
Statement	Specifies pass/fail criteria for the policy statement.
Display	Specifies how the policy statement is displayed: Ratio (x/y) , Percentage (%) , or Compliant/Non-Compliant .
Advanced	
Data Type	The type of data you want the ARC to analyze: Vulnerabilities or Events .
Base Filters	The filters used as the basis for data analysis. • If the Data Type is Vulnerabilities, you can select from the list of vulnerability analysis filter components.



Option	Description
	If the Data Type is Events, you can select from a list of event analysis filter components.
Compliant Filters	The filters used to determine the compliance conditions for the data analysis. For more information, see Vulnerability Analysis and Event Analysis. - If the Data Type is Vulnerabilities, you can select from the list of vulnerability analysis filter components. - If the Data Type is Events, you can select from a list of event analysis filter components. Note: Filters set in Base Filters are not present in Compliant Filters, with exception of the Assets and Plugin IDs. All filters set in Base Filters are carried over into Compliant Filters.
Compliant Condition	Specifies the conditions to match for determining compliance. For more information, see Vulnerability Analysis and Event Analysis. Specify a quantity: All, No, Any, > (greater than), < (less than), >= (greater than or equal to), and <= (less than or equal to). Specify hosts: Hosts, Vulnerabilities, and Ports.
Drilldown Filters	The filters to apply when clicking on the ARC policy statement for more details. For more information, see Vulnerability Analysis and Event Analysis. - If the Data Type is Vulnerabilities, you can select from the list of vulnerability analysis filter components. - If the Data Type is Events, you can select from a list of event analysis filter components.



Filters

You can apply filters on many pages of the Tenable.sc web interface to filter the data displayed on the page. After you build and apply a filter, the number next to the filter icon () updates to indicate the number of filters currently applied to the list.

You can build filters using one or more *filter components* with defined *filter component criteria*. Filter components are types of data (e.g., **CVE ID** or **Severity**). After you select a filter component, you specify the filter component criteria (e.g., a specific CVE ID or a specific severity level).

- [Vulnerability Analysis Filter Components](#)
- [Event Analysis Filter Components](#)
- [Mobile Analysis Filter Components](#)

For more information, see [Apply a Filter](#).

If you want to save a filter for repeated use, create a query, as described in [Queries](#).



Apply a Filter

Required User Role: Any

You can use filters to narrow the data displayed on specific pages. Some pages expand the filter options in the left side bar and some expand the filter options in the right side bar.

Each filterable page in Tenable.sc has a different set of filter components. On the **Vulnerability Analysis**, **Event Analysis**, and **Mobile Analysis** pages, you can add and remove filter components.

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

To filter data:

1. Log in to Tenable.sc 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. (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](#), [Event Analysis Filter Components](#), and [Mobile Analysis 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.

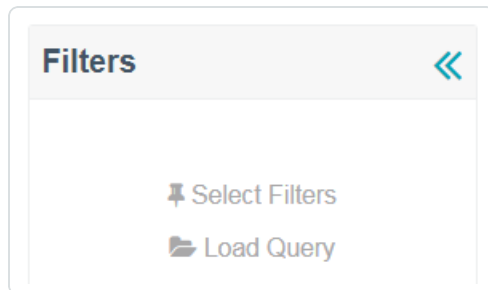
What to do next:

- (Optional) Save a filter on the **Vulnerability Analysis**, **Event Analysis**, and **Mobile Analysis** page as a reusable query, as described in [Add or Save a Query](#).

To filter data on a Tenable.sc page with a left side bar:

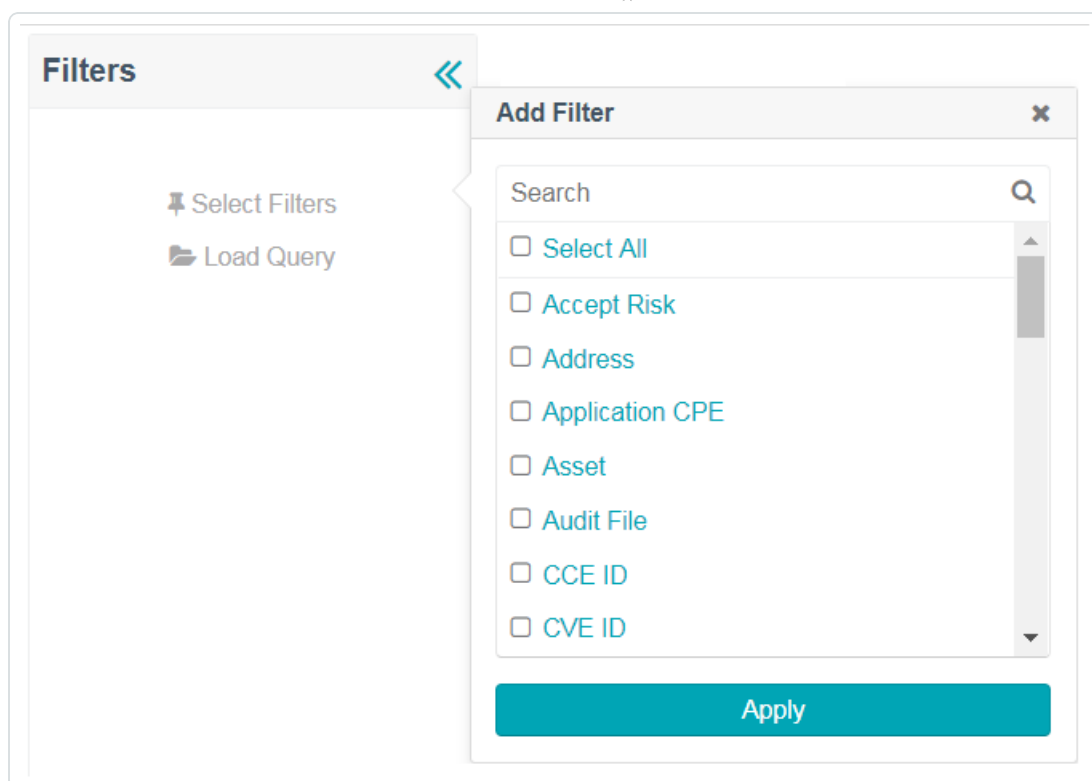
1. Log in to Tenable.sc via the user interface.
2. Navigate to any page that supports filtering.
3. On the left side of the page, click the double arrow (**>>**).

The **Filters** side bar expands.



4. Click **Select Filters**.

The filter components selection window appears.



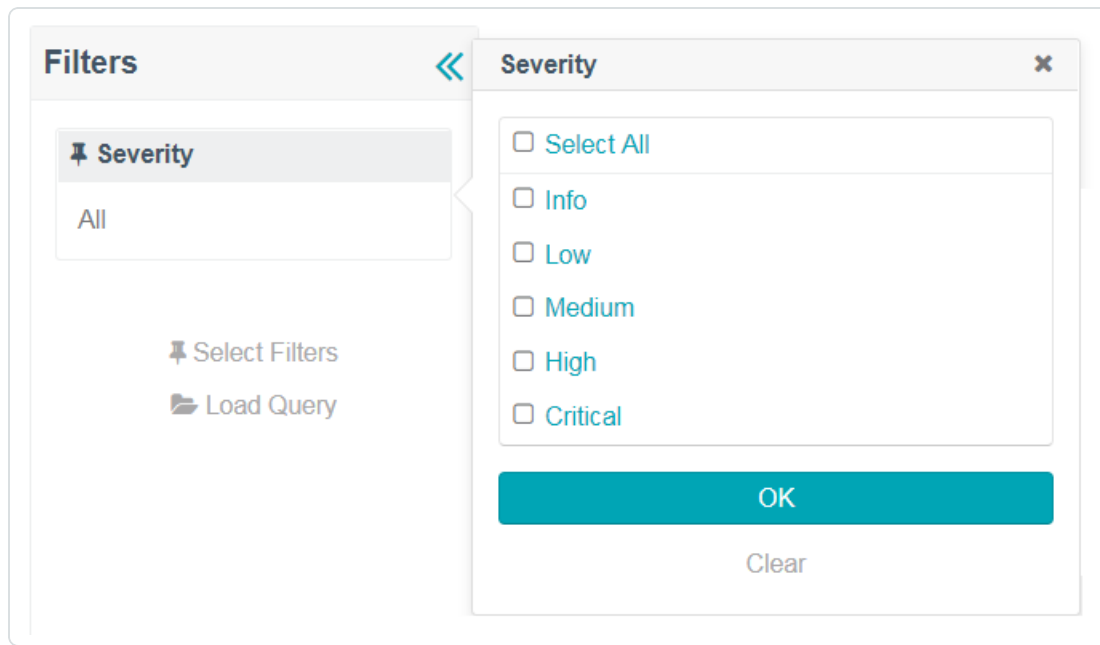
5. Select one or more filter component check boxes. For more information about the components supported for your analysis view, see [Vulnerability Analysis Filter Components](#), [Event Analysis Filter Components](#), and [Mobile Analysis Filter Components](#).

6. Click **Apply**.

The **Filters** side bar updates to show the filter components you selected.

7. Click the box for the filter component.

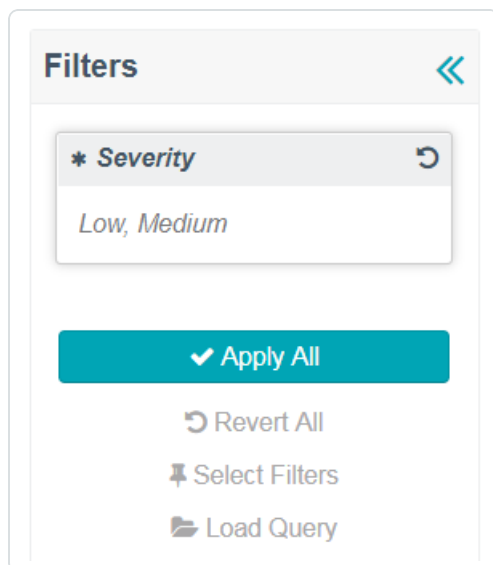
The filter component criteria selection window appears.



8. Modify the filter component criteria.

9. Click **OK**.

The **Filters** side bar updates to show the filter component criteria you modified. The **Apply All** button appears.



10. Click **Apply All**.

The page updates to reflect the filter you applied.



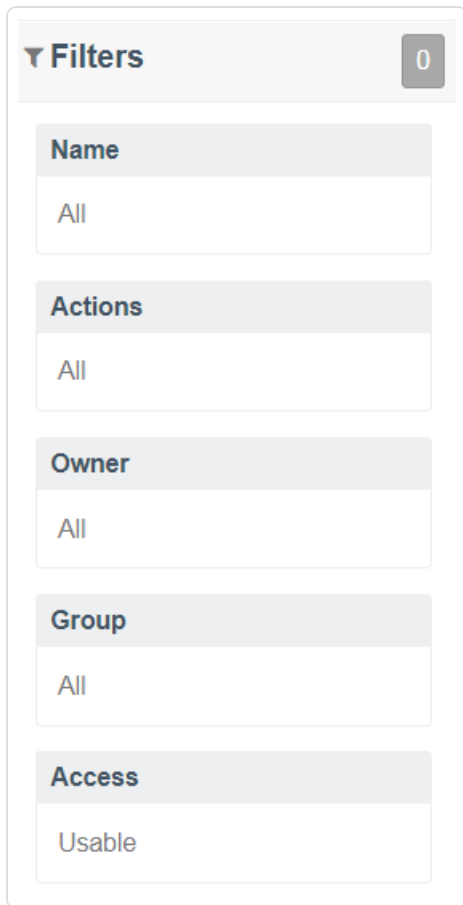
What to do next:

- (Optional) Save a filter on the **Vulnerability Analysis**, **Event Analysis**, and **Mobile Analysis** page as a reusable query, as described in [Add or Save a Query](#).

To filter data on a Tenable.sc page with an inline filter icon and right side bar:

1. Log in to Tenable.sc via the user interface.
2. Navigate to any page that supports filtering.
3. Locate the filter icon ().

The **Filters** side bar expands.



Filters
Name
All
Actions
All
Owner
All
Group
All
Access
Usable

4. Click the box for a filter component.

The filter component criteria selection window appears.



The screenshot shows a 'Filters' sidebar on the right side of the page. The sidebar has a header with the title 'Filters' and a count of '0'. Below the header, there are two filter components. The first component is titled 'Name' and contains a text input field with the placeholder text 'Enter Name', a teal 'Apply' button, and a 'Clear' button. The second component is titled 'Actions' and is currently empty.

5. Modify the filter component criteria.

6. Click **Apply**.

The **Filters** side bar updates to show the filter component criteria you modified. The page updates to reflect the filter you applied.



Queries

The Queries page displays a list of queries available for use. The information provided includes **Name**, **Type**, **Group**, **Owner**, and the **Last Modified** time. You can use a filter to narrow the list by any of the columns (except **Last Modified**). For more information, see [Filters](#).

To add a query, see [Add or Save a Query](#). To load a query, see [Load a Query](#).

Click on the **Query Name** to display an edit page and modify the selected query.

Query Options

Queries provide the ability to save custom views of vulnerability, event, ticket, user, and alert data for repeated access.

Option	Description
Name	A name for the query.
Description	A description for the query.
Tag	A tag for the query. For more information, see Tags .
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 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 Time-frame	Ticket creation date/time to filter against. Either specify an explicit time-frame, including the start and end time or choose one of the predefined periods (e.g., last 15 minutes, last hour, etc.)
Assigned Time-frame	Ticket assigned date/time to filter against. Either specify an explicit time-frame, including the start and end time or choose one of the predefined periods (e.g., last 15 minutes, last hour, etc.)
Modified Time-frame	Ticket modified date/time to filter against. Either specify an explicit time-frame, including the start and end time or choose one of the predefined periods (e.g., last 15 minutes, last hour, etc.)
Resolved Time-frame	Ticket resolution date/time to filter against. Either specify an explicit time-frame, including the start and end time or choose one of the predefined periods (e.g., last 15 minutes, last hour, etc.)
Closed Time-frame	Ticket closed date/time to filter against. Either specify an explicit time-frame, 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 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



Option	Description
	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 Evaluated Timeframe	Filters against the most recent alert evaluation 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.).



Add or Save a Query

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

You can add queries from the **Queries** page or from the **Vulnerability Analysis** page, **Event Analysis** page, or **Mobile Analysis** page. For more information about query options, see [Queries](#).

Note: If you want to create a mitigated vulnerabilities query, you must add the query from the **Vulnerability Analysis** page.

To add a query from the **Queries** page:

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

2. Click **Analysis > Queries**.

The **Queries** page appears.

3. Click **Add**.

4. Type a **Name** and **Description**.

5. (Optional) If you want to add a tag, type select a **Tag** from the drop-down. For more information, see [Tags](#).

6. Select a **Type**.

The **Tool** drop-down updates with options for that type.

7. Select a **Tool**.

8. Click **Add Filter**.

The **Filters** section expands. For more information, see [Filters](#).

9. Select a filter component from the **Select a Filter** drop-down.

The filter component criteria box appears.

10. In the filter component criteria box, type or select filter component criteria.

11. Click the  button.

The filter component is added.



12. (Optional) To add other filter components, repeat step 8.
13. Click **Submit**.

Tenable.sc saves your configuration.

To save a query from an analysis page:

1. Log in to Tenable.sc via the user interface.
2. Do one of the following to navigate to an analysis page:
 - Click **Analysis > Vulnerabilities**
 - 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. In the **Options** drop-down box, click **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 tag, type or select a **Tag** from the drop-down. For more information, see [Tags](#).
8. Click **Submit**.

Tenable.sc saves your configuration.



Load a Query

Required 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.sc via the user interface.
2. Navigate to any page that supports filtering.
3. On the left side of the page, click the double arrow (**>>**).

The **Filters** side bar expands.

4. On the left side of the page, click the filter icon ().

The filter panel appears.

5. Click **Load Query**.
6. Select the query you want to load.
7. Click **Apply**.

The page updates, filtered by the query you selected.



Workflow Actions

Workflow actions allow organizational users to configure and manage alerting, ticketing, and accept risk or recast risk rules. These functions allow the user to be notified of and properly handle vulnerabilities and events as they come in.

For more information, see [Alerts](#), [Tickets](#), [Accept Risk Rules](#), and [Recast Risk Rules](#).



Alerts

Tenable.sc can be configured to perform actions, such as email alerts, for select vulnerability or alert occurrences to various users regardless of whether the events correlate to a local vulnerability or not. Other alert actions include UI notification, ticket creation/assignment, remediation scans, launching a report, email notification, and syslog alerting. Many actions can be assigned per ticket.

Click the  menu to add an Alert from the main Alerts page. Here you can, **Edit**, **Evaluate**, **View** (view details of), and **Delete** alerts. The **Evaluate** option allows an alert to be tested whether it has met the configured time criteria or not. Clicking on an alert will take the user to the Edit Alert page for the selected alert.

Alert Options

Option	Description
General	
Name	Alert name
Description	Descriptive text for the alert
Schedule	The setting will determine how often the alert checks for the conditions to be matched. Selections vary in frequency from 15 minutes to monthly. Selecting the option of Never will create the alert to be launched only on demand.
Behavior	If set to alert on the first occurrence, the alert will only trigger when the condition initially changes from false to true. The other option is to trigger on each detection of the true condition.
Condition	
Type	Vulnerability , Event , or Ticket .
Trigger	• IP Count – Trigger on vulnerabilities or events whose IP address count matches the given parameters. • Unique Vulnerability/Event Count – Trigger an alert when the vulnerability/event count matches the given parameters. This option is



Option	Description
General	
	set to Unique Vulnerability Count for vulnerability alerts and Event Count for event alerts. • Port Count – Trigger an alert when the events/vulnerabilities using a certain port number match the given parameters.
Query	The dataset to which the trigger condition will be compared.
Filters	Apply advanced filters to the vulnerability or event data. The complete filter set may be created here, or if a Query was selected those parameters may be edited. For more information, see Filters.
Actions	
Add Actions	Adding actions will determine what the alert does with triggered events. The options are Assign Ticket, Email, Generate Syslog, Launch Scan, Launch Report, or Notify Users. Multiple actions may be triggered for each alert. For more information, see Alert Actions.



Alert Actions

Tenable.sc automatically performs *alert actions* when an alert triggers. You can configure the following types of alert actions:

- [Assign Ticket](#)
- [Email](#)
- [Generate Syslog](#)
- [Launch Scan](#)
- [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.sc 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 will receive the ticket	--

Email

When the alert triggers, Tenable.sc 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%, this specifies the unique identification number assigned to the alert by Tenable.sc. • Alert name – Designated with the variable: %alertName%, this specifies the name assigned to the alert (e.g., “Test email alert”). • Trigger Name – Designated with the variable: %triggerName%, this specifies if the trigger is IP address count, Vulnerability count, or Port count. • Trigger Operator – Designated with the variable: %triggerOperator%, this specifies which operator was used for the count: >=, =, <= or != • Trigger value – Designated with the variable: %triggerValue%, this specifies the specific threshold value set that will trigger 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.sc. • Alert owner – Designated with the variable: %owner%, this specifies the user that created the alert.	(see description)



	• SC URL – Designated with the variable: %url%, this specifies the URL that the Tenable.sc can be accessed with. This is useful where the URL that users can access Tenable.sc with differs from the URL known by Tenable.sc. The sample email alert below contains some of these keywords embedded into an HTML email: Alert %alertName% (id #%alertID%) has triggered. Alert Definition: %triggerName% %triggerOperator% %triggerValue% Calculated Value: %calculatedValue% Please visit your Tenable.sc (%url%) for more information. This e-mail was automatically generated by Tenable.sc as a result of alert %alertName% owned by %owner%. If you do not wish to receive this email, contact the alert owner.	
Include Results	When enabled, Tenable.sc 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.sc 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.sc 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.sc sends with the syslog alert.	--

Launch Scan

When the alert triggers, Tenable.sc launches an active scan from an existing active scan template. The active scan **Schedule** must be **On Demand**. For more information, see [Active Scans](#) and [Active Scan Settings](#).

Option	Description	Default
Scan	(Required) The scan template Tenable.sc uses for the alert scan. Note: Tenable.sc scans the host that triggered the scan, not the host within the scan template. IPs used for the scan targets are limited to the top 100 results of the alert query.	--

Launch Report



When the alert triggers, Tenable.sc generates a report from an existing report template. For more information, see [Reports](#).

Option	Description	Default
Report Template	(Required) The report template Tenable.sc uses to generate a report based on the triggered alert data.	--

Notify Users

When the alert triggers, Tenable.sc displays a notification to the specified users.

Option	Description	Default
Message	(Required) The notification message Tenable.sc sends when the alert triggers.	--
Users	(Required) The users who receive the notification message.	--



Tickets

Tickets can be created both manually and automatically by a predefined set of conditions through the alerting functionality described above.

For more information, see [Open a Ticket](#).

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 • 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.



Option	Description
Query Views	
Add Query View	Click to choose a query for the ticket assignee to help provide context for coming up with a resolution.

In addition to adding and editing tickets, a **Browse** command button is available. This option enables the user to view the vulnerability snapshot added during ticket creation. The displayed view matches the query that was used by the ticket.

To view details about an existing ticket, click the ticket to bring up the edit ticket page, use the **Edit** option from the  menu to view options that were set during the **Add Ticket** process or use the **View** option from the  menu to view a Ticket Detail summary with the name, status, creator, assignee, history, queries, description, and ticket notes.

Once a ticket has been mitigated, click **Resolve** from the  menu to provide ticket resolution.

Once the ticket is resolved it may be closed from the **Close** option from the  menu.

Within the **Status** drop-down box, the user can select from one of these status options: Assigned, Resolved, More Information, Duplicate, or Not Applicable. Choose the correct status and add notes relevant to the ticket resolution. Resolved tickets still show up in the user's ticket queue with an **Active** status. Closing a ticket removes the ticket from the **Active** status filter view, but does not provide the ability to add notes similar to the **Update Ticket** function. Tickets in the **Resolved** or **Closed** state can always be reopened as needed.



Open a Ticket

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

You can use tickets within Tenable.sc to coordinate the assessment and remediation of vulnerabilities and security events.

You can configure a ticket from an analysis page, or from the **Tickets** page. For more information about the options to configure, see [Tickets](#).

To open a ticket from an analysis page:

1. Log in to Tenable.sc via the user interface.
2. Click **Analysis > Vulnerabilities** or **Analysis > Events**.
The **Vulnerability Analysis** or **Event Analysis** page appears.
3. In the upper-right corner, click the **Options** drop-down box.
4. Click **Open Ticket**.
5. In the **Name** box, type a name.
6. (Optional) In the **Description** box, type a description.
7. (Optional) In the **Notes** box, type a note to the assignee.
8. In the **Assignee** drop-down box, select an assignee.
9. In the **Classification** drop-down box, select a classification.
10. Click **Submit**.

Tenable.sc creates the ticket.

To open a ticket from the Tickets page:

1. Log in to Tenable.sc via the user interface.
2. Click **Workflow > Tickets**.

The **Tickets** page appears.

3. Click **Add**.



4. In the **Name** box, type a name.
5. (Optional) In the **Description** box, type a description.
6. (Optional) In the **Notes** box, type a note to the assignee.
7. In the **Assignee** drop-down box, select an assignee.
8. In the **Classification** drop-down box, select a classification.
9. (Optional) Click **Add Query View**.
10. Click **Submit**.

Tenable.sc creates the ticket.



Accept Risk Rules

The Accept Risk Rules page displays a list of accept risk rules configured in Tenable.sc. Organizational users must add accept risk rules before the rules appear on this page. For more information, see [Add an Accept Risk Rule](#).

Adding a rule moves vulnerabilities from the unfiltered cumulative database view. These vulnerabilities are not deleted, but only display in the cumulative database vulnerability view if the **Accepted Risk** filter option is checked. For more information, see [Filters](#).

Administrator and organizational users can manage accept risk rules. You can access information on what particular vulnerabilities or hosts have been declared to be accepted and, if noted in the comments, the reason.

To view details for a rule, click the row. To delete a rule, see [Delete an Accept Risk Rule](#).



Add an Accept Risk Rule

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

If you create an accept risk rule, any vulnerabilities that match the rule are automatically accepted. Risk accepted vulnerabilities do not appear in a vulnerability search if your filter excludes **Accepted Risk** vulnerabilities.

For more information, see [Accept Risk Rules](#).

To add an accept risk rule:

1. Log in to Tenable.sc via the user interface.
2. Click **Analysis > Vulnerabilities**.

The **Vulnerability Analysis** page appears.

3. Click the analysis tools drop-down box and select **Vulnerability Detail List**, **Vulnerability List**, or **Vulnerability Summary**.

The page refreshes to show the analysis tool view you selected.

4. In the row for the vulnerability for which you want to accept risk, click the  menu.

The actions menu appears.

5. Click **Accept Risk**.
6. (Optional) In the **Comment** box, add a comment.
7. (Optional) In the **Expires** box, select the date you want the accept risk rule to expire.
8. In the **Repository** section, select one or more repositories where you want to apply the rule.
9. Click **Submit**.

Tenable.sc saves your configuration.

Note: There can be a short delay between clicking on **Submit** and vulnerabilities showing the new risk acceptance. It may be necessary to reload the filters to view the applied changes.



Delete an Accept Risk Rule

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

You can delete an accept risk rule to stop accepting the risk associated with a vulnerability.

To delete an accept risk rule:

1. Log in to Tenable.sc.
2. Click **Workflow > Accept Risk Rules** (Organizational users) or **Repositories > Accept Risk Rules** (Administrator users).

The **Accept Risk Rules** page appears.

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

The actions menu appears.

4. Click **Delete**.

A confirmation window appears.

5. Click **Delete**.

Tenable.sc deletes the rule.

6. Click **Apply Rules**.

Tenable.sc stops accepting the risk associated with the vulnerability.



Recast Risk Rules

The Recast Risk Rules page displays a list of recast risk rules configured in Tenable.sc. Organizational users must add recast risk rules before the rules appear on this page. For more information, see [Add a Recast Risk Rule](#).

Administrator and organizational users can manage recast risk rules. You can access information on what particular vulnerabilities or hosts have had risk levels recast, their new severity level and, if noted in the comments, the reason for the severity change. Rules may be searched by Plugin ID or Repository.

To view details for a rule, click the row. To delete a rule, see [Delete a Recast Risk Rule](#).



Add a Recast Risk Rule

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

If you create a recast risk rule, any vulnerabilities that match the rule are automatically set to the severity you specified in the rule.

For more information, see [Recast Risk Rules](#).

To add a recast risk rule:

1. Log in to Tenable.sc via the user interface.
2. Click **Analysis > Vulnerabilities**.

The **Vulnerability Analysis** page appears.

3. Click the analysis tools drop-down box and select **Vulnerability Detail List**, **Vulnerability List**, or **Vulnerability Summary**.

The page refreshes to show the analysis tool view you selected.

4. In the row for the vulnerability you want to recast, click the  menu.

The actions menu appears.

5. Click **Recast Risk**.
6. In the **New Severity** drop-down box, select a new severity for the vulnerability.
7. (Optional) In the **Comment** box, add a comment.
8. In the **Repository** section, select one or more repositories where you want to apply the rule.
9. Click **Submit**.

Tenable.sc saves your configuration.

Note: There can be a short delay between clicking on **Submit** and vulnerabilities showing the new risk. It may be necessary to reload the filters to view the applied changes.



Delete a Recast Risk Rule

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

You can delete a recast risk rule to remove your custom severity for a vulnerability. Then, if Tenable.sc sees the vulnerability again, the vulnerability receives the severity currently associated with the plugin.

To delete a recast risk rule and remove your custom severity:

1. Log in to Tenable.sc.
2. Click **Workflow > Recast Risk Rules** (Organizational users) or **Repositories > Recast Risk Rules** (Administrator users).

The **Recast Risk Rules** page appears.

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

The actions menu appears.

4. Click **Delete**.

A confirmation window appears.

5. Click **Delete**.

Tenable.sc deletes the rule.

6. Click **Apply Rules**.

If Tenable.sc sees the vulnerability again, the vulnerability receives the severity currently associated with the plugin.



Additional Resources

The topics in this section offer guidance in areas related to Tenable.sc.

- [Start, Stop, or Restart Tenable.sc](#)
- [License Declarations](#)
- [Encryption Strength](#)
- [File and Process Allow List](#)
- [Manual LCE Key Exchange](#)
- [Manual Nessus SSL Certificate Exchange](#)
- [Offline Tenable.sc Plugin and Feed Updates](#)
- [Troubleshooting](#)



Start, Stop, or Restart Tenable.sc

Required User Role: Root user

When Tenable.sc is installed, the required services are started by default.

To change the status of Tenable.sc:

1. Log in to Tenable.sc via the command line interface (CLI).
2. In the CLI in Tenable.sc, run the following command to check the status of your Tenable.sc:

```
# service SecurityCenter status
```

The system indicates whether Tenable.sc is running or stopped.

3. Run one of the following commands to change the status of your Tenable.sc:

- To start Tenable.sc, run:

```
# service SecurityCenter start
```

- To stop Tenable.sc, run:

```
# service SecurityCenter stop
```

- To restart Tenable.sc, run:

```
# service SecurityCenter restart
```



License Declarations

Tenable.sc's Software License Agreement can be found on Tenable.sc in the `/opt/sc/docs` directory.

For a list of third-party software packages that Tenable utilizes with Tenable.sc, see [Tenable Third-Party License Declarations](#).



Encryption Strength

Tenable.sc 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.sc and clients (Tenable.sc users).	SSL/TLS 1.2 with the strongest encryption method supported by Tenable.sc Apache and your browser, CLI program, or API program: ECDHE+AESGCM, EDH+AESGCM, AES256+ECDHE, or AES256+EDH. For more information about strong encryption, see Configure SSL/TLS Strong Encryption .
Communications between Tenable.sc and the Tenable product registration server.	SSL/TLS 1.2 with ECDHE-RSA-AES256-GCM-SHA384
Communications between Tenable.sc and the Tenable plugin update server.	SSL/TLS 1.2 with ECDHE-RSA-AES256-GCM-SHA384
Communications between Tenable.sc	SSL/TLS 1.2 with the strongest encryption method supported by Tenable.sc Apache and your browser, CLI program, or API program:



Function	Encryption
and: • Nessus or Nessus Manager • Tenable.io • NNM • LCE	ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-SHA384, or ECDHE-RSA-AES256-GCM-SHA384.
Synchronizations between Tenable.sc and Tenable.io for Lumin.	SSL/TLS 1.2



Configure SSL/TLS Strong Encryption

You can configure SSL/TLS strong encryption for Tenable.sc-client communications to meet the security needs of your organization. For more information about Tenable.sc encryption, see [Encryption Strength](#).

To configure SSL/TLS strong encryptions for Tenable.sc communications:

1. Open the `/opt/sc/support/conf/sslciphers.conf` file in a text editor.
2. Add the following content at the end of the file:

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

Tenable.sc 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.



Configure Tenable.sc for NIAP Compliance

If your organization requires that your instance of Tenable.sc meets National Information Assurance Partnership (NIAP) standards, you can configure relevant settings to be compliant with NIAP standards.

You must run Tenable.sc 5.15.0 or later to fully configure Tenable.sc for NIAP compliance. If you are running Tenable.sc 5.15.0, you must install a patch to configure Tenable.sc for NIAP compliance. Contact Tenable Support for assistance with the required patch. For more information about upgrading Tenable.sc, see [Before You Upgrade](#) and [Upgrade Tenable.sc](#).

For more information about Tenable.sc storage and communications encryption, see [Encryption Strength](#).

Before you begin:

- If you are running Tenable.sc 5.15.0, contact Tenable Support for assistance with the required patch.
- If you are using SSL certificates to log in to Tenable.sc, ensure your server and client certificates are NIAP-compliant. For more information about certificate authentication, see [Certificate Authentication](#).
- Confirm you have enabled the full disk encryption capabilities provided by the operating system on the host where Tenable.sc is installed.

To configure Tenable.sc for NIAP compliance:

1. Log in to Tenable.sc via the command line interface (CLI).
2. In the CLI in Tenable.sc, as the root or tns user, run the following commands to configure strong SSL/TLS encryption for Tenable.sc communications:

```
# /opt/sc/support/bin/sqlite3 /opt/sc/application.db "INSERT INTO Configuration ( type,name,value,visible,editable ) VALUES ( 64, 'SSLVersion', 'TLSv1_2', 'false', 'false' )"
```




```
# /opt/sc/support/bin/sqlite3 /opt/sc/application.db "INSERT INTO Configuration ( type,name,value,visible,editable ) VALUES ( 64, 'SSLCipherList', 'ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES256-GCM-SHA384', 'false', 'false' )"
```

3. Configure the Tenable.sc web server to use strong encryption for storage and communications, as described in [Configure SSL/TLS Strong Encryption](#).

Note: For NIAP compliance, you must configure TLS 1.2 encryption with any of the following ciphers: ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-SHA384, or ECDHE-RSA-AES256-GCM-SHA384.

4. If you connect Tenable.sc to Nessus, Nessus Manager, Nessus Network Monitor, or Log Correlation Engine, you must use certificates to authenticate the connection. For more information, see [Manual Nessus SSL Certificate Exchange](#) and [Manual LCE Key Exchange](#).



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.sc to the allow list.

If you configured supporting resources for Tenable.sc, 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.sc, see [Resources](#).

Tenable recommends allowing the following Tenable.sc files and processes.

Allow List
Files
/opt/sc/*
Processes
/opt/sc/bin/*
/opt/sc/src/*
/opt/sc/support/bin/*
/opt/sc/www/*



Manual LCE Key Exchange

Required User Role: Administrator

You are not normally required to make a manual key exchange between Tenable.sc and the LCE; however, in some cases where you are prohibited from remote root login or required to do key exchange debugging, you must manually exchange the keys.

For the remote LCE to recognize Tenable.sc, copy the SSH public key of Tenable.sc and append it to the `/opt/lce/.ssh/authorized_keys` file. The `/opt/lce/daemons/lce-install-key.sh` script performs this function.

Note: The LCE server must have a valid license key installed and the LCE daemon must be running before you perform the steps below.

To perform manual LCE key exchange:

1. Log in to Tenable.sc via the user interface.
2. Download the Tenable.sc key, as described in [Download the Tenable.sc SSH Key](#).
3. Save the file locally as **SSHKey.pub**.

Caution: Do not edit the file or save it to any specific file type.

4. From the workstation where you downloaded the key file, use a secure copy program (e.g., WinSCP) to copy the **SSHKey.pub** file to the LCE system.

Note: You must have the credentials of an authorized user on the LCE server to perform this step.

For example, if you have a user **username** configured on the LCE server (hostname **lceserver**) whose home directory is **/home/username**, the command on a Unix system is as follows:

```
# scp SSHKey.pub username@lceserver:/home/username
```

5. After you copy the file to the LCE server, in the CLI, run the following command to move the file to `/opt/lce/daemons`:



```
# mv /home/username/SSHKey.pub /opt/lce/daemons
```

6. On the LCE server, as the root user, run the following command to change the ownership of the SSH key file to `lce`:

```
# chown lce /opt/lce/daemons/SSHKey.pub
```

7. Run the following command to append the SSH public key to the **`/opt/lce/.ssh/authorized_keys`** file:

```
# su lce
# /opt/lce/daemons/lce-install-key.sh /opt/lce/daemons/SSHKey.pub
```

8. To test the communication, as the user `tns` on the Tenable.sc system, attempt to run the `id` command:

```
# su tns
# ssh -C -o PreferredAuthentications=publickey lce@<LCE-IP> id
```

If you have not previously established a connection, a warning appears that is similar to the following:

```
The authenticity of host '198.51.100.28 (198.51.100.28)' can't be established.
RSA key fingerprint is 86:63:b6:c3:b4:3b:ba:96:5c:b6:d4:42:b5:45:37:7f.
Are you sure you want to continue connecting (yes/no)?
```

9. Answer `yes` to this prompt.

If the key exchange worked correctly, a message similar to the following appears:

```
# uid=251(lce) gid=251(lce) groups=251(lce)
```

10. You can add the IP address of Tenable.sc to the LCE system's `/etc/hosts` file. This prevents the SSH daemon from performing a DNS lookup that can add seconds to your query times.



11. You can add the LCE to Tenable.sc via the normal administrator process, described in [Log Correlation Engines](#).



Manual Nessus SSL Certificate Exchange

If you want to use self-signed certificates for the Tenable.sc-Nessus connection, you can perform manual Nessus SSL certificate exchange.

Caution: Please note that users should be familiar with PKI deployments and it is not recommended that the Nessus server be used as the site's PKI system. The method described here is intended to assist in testing the functionality of the certificate exchange to assist users in the incorporation of the certificates into their current PKI system. In this method, the same key is shared between multiple servers. This may not be acceptable in some installations.

- [Overview of Nessus SSL Certificates and Keys](#)
- [Nessus Certificate Configuration for Unix](#)
- [Nessus Certificate Configuration for Windows](#)



Overview of Nessus SSL Certificates and Keys

Nessus supports authentication protocols based on the OpenSSL toolkit (for more information about the toolkit, see <http://www.openssl.org/>). This provides cryptographic protection and secure authentication.

In the example described in this document, there are three key system components: the certificate authority, the Nessus server and the Nessus client (Tenable.sc). It is necessary to generate the keys required for the SSL communication and copy them to the appropriate directories.

Certificate Authority

The certificate authority (CA) ensures that the certificate holder is authentic and not an impersonator. The CA holds a copy of the certificates for registered users to certify that the certificate is genuine. When the CA receives a certificate signing request (CSR), it validates and signs the certificate.

In the example provided in this document, the CA resides on the Nessus server (which is not the recommended method for a production environment). In a proper PKI deployment, the CA would be a separate system or entity, such as Thawte or Verisign.

Nessus Server

In the example described in this document, the Nessus server is the same physical system that holds the CA, but this will not likely be the case in a production environment. The Nessus server is the target of the secure communication and its keys must be generated locally and copied to the systems that will need to communicate with it using the SSL protocol. The Nessus server has users defined that authenticate to it either by simple login and password or via SSL. These users will also have keys associated with them.

Nessus Client (Tenable.sc)

The Nessus client, Tenable.sc, communicates with the Nessus server via SSL. It uses keys generated for a Nessus client and stores these keys and the certificate for the CA in the `/opt/sc/daemons` directory. These keys must be owned by the “tns” userid.



Nessus Certificate Configuration for Unix

The following topic describes the commands and relevant files involved in the Nessus SSL process on a Red Hat Linux system. This process creates the following files:

File Name Created	Purpose	Where to Copy to
/opt/nessus/com/nessus/CA/cacert.pem	This is the certificate for the Certificate Authority. If using an existing PKI, this will be provided to you by the PKI and must be copied to this location.	/opt/nessus/com/nessus/CA on the initial Nessus server and any additional Nessus servers that need to authenticate using SSL.
/opt/nessus/com/nessus/CA/servercert.pem	This is the public certificate for the Nessus server that is sent in response to a CSR.	/opt/nessus/com/nessus/CA on any additional Nessus servers that need to authenticate using SSL.
/opt/nessus/var/nessus/CA/cakey.pem	This is the private key of the Certificate Authority. It	/opt/nessus/var/nessus/CA on any additional Nessus servers that need to authenticate using SSL.



File Name Created	Purpose	Where to Copy to
	may or may not be provided by the Certificate Authority, depending on if they allow the creation of sub users.	
/opt/nessus/var/nessus/CA/serverkey.pem	This is the private key of the Nessus server.	/opt/nessus/var/nessus/CA on any additional Nessus servers that need to authenticate using SSL.

Create Nessus Client Keys

The Nessus user, in this case the user ID that Tenable.sc uses to communicate with the Nessus server, is created by the following command:

```
# /opt/nessus/sbin/nessuscli mkcert-client
```

This command creates the keys for the Nessus clients and optionally registers them appropriately with the Nessus server by associating a distinguished name (dname) with the user ID. It is important to respond **y** (yes) when prompted to register the user with the Nessus server for this to take effect. The user name may vary and is referred to here as **user**.

The certificate filename is a concatenation of **cert_**, the user name you entered and **.pem**. Additionally, the key filename is a concatenation of **key_**, the user name you entered and **.pem**.

If the user was previously added via the `/opt/nessus/sbin/nessuscli adduser` command, you will still need to run this program to register the user. If you have not previously created the user, it



is not necessary to also run the `nessuscli adduser` command; the user is created if it does not already exist. The following files are created by this command:

File Name Created	Purpose
/tmp/nessus-xxxxxxx/cert_{user-}.pem	This is the public certificate for the specified user.
/tmp/nessus-xxxxxxx/key_{user-}.pem	This is the private key for the specified user.
/opt/nessus/var/nessus/users/{user}/auth/dname	This is the distinguished name to be associated with this user. The distinguished name consists of a number of options separated by commas in the following format: /C={country}/ST={state}/L={location}/OU={organizational unit}/O={organization}/CN={common name}

Create and Deploy SSL Authentication for Nessus

An example SSL Certificate configuration for Nessus to Tenable.sc authentication is included below:

In the example described here, Tenable.sc and the Nessus scanner are defined as follows. Your configuration varies:

Tenable.sc:

IP: 192.0.2.50

OS: Red Hat ES 5

Nessus Scanner:

IP: 192.0.2.202

OS: Red Hat ES 5

Create Keys and User on Nessus Server

Log in to the Nessus scanner and use the `su` command to become the root user. Create the Certificate Authority and Nessus server certificate as follows:



```
# /opt/nessus/sbin/nessuscli mkcert
```

Creation of the Nessus SSL Certificate

This script will now ask you the relevant information to create the SSL certificate of Nessus. Note that this information will **NOT** be sent to anybody (everything stays local), but anyone with the ability to connect to your Nessus daemon will be able to retrieve this information.

CA certificate life time in days [1460]:

Server certificate life time in days [365]:

Your country (two letter code) [US]:

Your state or province name [NY]:

Your location (e.g. town) [New York]:

Your organization [Nessus Users United]: Tenable Network Security

This host name [Nessus4_2]:

Congratulations. Your server certificate was properly created.

The following files were created :

. Certification authority :



```
Certificate = /opt/nessus//com/nessus/CA/cacert.pem
```

```
Private key = /opt/nessus//var/nessus/CA/cakey.pem
```

. Nessus Server :

```
Certificate = /opt/nessus//com/nessus/CA/servercert.pem
```

```
Private key = /opt/nessus//var/nessus/CA/serverkey.pem
```

Next, create the user ID for the Nessus client, which is Tenable.sc in this case, to log in to the Nessus server with, key and certificate. This is done with the command `/opt/nessus/sbin/nessuscli mkcert-client`. If the user does not exist in the Nessus user database, it is created. If it does exist, it is registered to the Nessus server and have a distinguished name (dname) associated with it. It is important to respond **y**(yes) when prompted to register the user with the Nessus server for this to take effect. The user must be a Nessus admin, so answer **y** when asked. The following example shows the prompts and typical answers:

```
# /opt/nessus/sbin/nessuscli mkcert-client
```

```
Do you want to register the users in the Nessus server
```

```
as soon as you create their certificates ? [n]: y
```

```
-----  
Creation Nessus SSL client Certificate  
-----
```

```
This script will now ask you the relevant information to create the SSL  
client certificates for Nessus.
```

```
Client certificate life time in days [365]:
```



Your country (two letter code) [FR]: US

Your state or province name []: MD

Your location (e.g. town) [Paris]: Columbia

Your organization []: Tenable Network Security

Your organizational unit []:

We are going to ask you some question for each client certificate

If some question have a default answer, you can force an empty answer by entering a single dot '.'

User #1 name (e.g. Nessus username) []: paul

User paul already exists

Do you want to go on and overwrite the credentials? [y]: y

Should this user be administrator? [n]: y

Country (two letter code) [US]:

State or province name [MD]:

Location (e.g. town) [Columbia]:

Organization [Tenable Network Security]:

Organizational unit []:

e-mail []:

User rules



nessusd has a rules system which allows you to restrict the hosts that \$login has the right to test. For instance, you may want him to be able to scan his own host only.

Please see the `nessus-adduser(8)` man page for the rules syntax

Type the rules for this user, and enter a BLANK LINE once you are done:
(the user can have an empty rules set)

User added to Nessus.

Another client certificate? [n]: n

Your client certificates are in `/tmp/nessus-043c22b5`

You will have to copy them by hand

#

The certificates created contain the username entered previously, in this case paul, and are located in the directory as listed in the example above (e.g., `/tmp/nessus-043c22b5`).

Create the `nessuscert.pem` Key

In the above specified tmp directory, the certificate and key files in this example are named `cert_paul.pem` and `key_paul.pem`. These files must be concatenated to create `nessuscert.pem` as follows:

```
# cd /tmp/nessus-043c22b5  
  
# cat cert_paul.pem key_paul.pem > nessuscert.pem
```

Note: The `nessuscert.pem` file is used when configuring the Nessus scanner on Tenable.sc. This file needs to be copied to somewhere accessible for selection from your web browser during the Nessus configuration.

Configure Nessus Daemons



To enable certificate authentication on the Nessus server, the **force_pubkey_auth** setting must be enabled. Once enabled, log in to the Nessus server may only be completed by SSL certificates. Username and password login are disabled. As the root (or equivalent) user on the Nessus server, run the following command:

```
# /opt/nessus/sbin/nessuscli fix --set force_pubkey_auth=yes
```

Restart the Nessus daemons with the appropriate command for your system. The example here is for Red Hat:

```
# /sbin/service nessusd restart
```

Change the Nessus Mode of Authentication

In Tenable.sc, update your Nessus scanner configuration to use SSL certificate-based authentication. For more information, see [Add a Nessus Scanner](#).

Edit Nessus Scanner

General

Name*

Nessus Scanner

Description

Host*

nessus.example.com

Port*

8834

Enabled

☒

Verify Hostname

☐

Use Proxy

☐

Authentication

Type

SSL Certificate

Certificate*

nessuscert.pem

✕ Cancel

Considerations for Custom Certificates



During an upgrade, Tenable.sc will check for the presence of custom SSL certificates. If certificates are found and the owner is not Tenable, any newly generated certificates will be named with a **.new** extension and placed in the `/opt/sc/support/conf` directory to avoid overwriting existing files.

Deploy to Other Nessus Scanners

After you configure authentication on one Nessus scanner, you can use the same SSL certificates and user names to authenticate other Nessus scanners.

Before you begin:

- Set up and configure all of your Nessus scanners.
- Add your Nessus scanners to Tenable.sc, as described in [Add a Nessus Scanner](#).

To duplicate the same authentication configuration on other Nessus scanners:

1. In the command line interface (CLI) on another Nessus server, run the following command to copy the certificate files onto your other Nessus server:

```
# cd /opt/nessus/var/nessus/CA  
  
# scp cakey.pem serverkey.pem root@nessusIP:/opt/nessus/var/nessus/CA  
  
# cd /opt/nessus/com/nessus/CA  
  
# scp cacert.pem servercert.pem root@nessusIP:/opt/nessus/com/nessus/CA
```

2. Run the following command to create a user directory on your second Nessus server, using the same name as [the user you created on the first Nessus server](#). Replace *admin* with the user's name:

```
/opt/nessus/sbin/nessuscli adduser admin
```

A confirmation prompt appears.

3. Press *y* to confirm you want the user to have system administrator privileges.

Nessus creates the user.



4. Run the following command to copy the [the user you created on the first Nessus server](#) to the directory you created in step 2. Replace *admin* with the user's name:

```
# cd /opt/nessus/var/nessus/users  
  
# tar -zcvf - admin | ssh -C root@nessusIP "tar -zxvf - -C /opt/nessus/var/nessus/users"
```

5. Run the following command to force Nessus to authenticate via certificate:

```
/opt/nessus/sbin/nessuscli fix --set force_pubkey_auth=yes
```

6. Restart the Nessus service on all the Nessus servers with the appropriate command for your system. This example is for Red Hat:

```
# /sbin/service nessusd restart
```

7. In Tenable.sc, update all of your Nessus scanner configurations to use SSL certificate-based authentication. For more information, see [Add a Nessus Scanner](#).



Nessus Certificate Configuration for Windows

Commands and Relevant Files

The following section describes the commands and relevant files involved in the Nessus SSL process on a Windows system.

Certificate Authority and Nessus Server Certificate

The command `C:\Program Files\Tenable\Nessus\nessuscli mkcert` creates the Certificate Authority and generates the server certificate. This command creates the following files:

File Name Created	Purpose	Where to Copy to
C:\Program Files\Tenable\Nessus\nessus\CA\cacert.pem	This is the certificate for the Certificate Authority. If using an existing PKI, this will be provided to you by the PKI and must be copied to this location.	C:\Program Files\Tenable\Nessus\nessus\CA\ on any additional Nessus servers that need to authenticate using SSL.
C:\Program Files\Tenable\Nessus\nessus\CA\servercert.pem	This is the public certificate for the Nessus server that	C:\Program Files\Tenable\Nessus\nessus\CA\ on any additional Nessus servers that need to authenticate using SSL.



File Name Created	Purpose	Where to Copy to
	is sent in response to a CSR.	
C:\Program Files\Tenable\Nessus\nessus\CA\cakey.pem	This is the private key of the Certificate Authority. It may or may not be provided by the Certificate Authority, depending on if they allow the creation of sub users.	C:\Program Files\Tenable\Nessus\nessus\CA\ on any additional Nessus servers that need to authenticate using SSL.
C:\Program Files\Tenable\Nessus\nessus\CA\serverkey.pem	This is the private key of the Nessus server.	C:\Program Files\Tenable\Nessus\nessus\CA\ on any additional Nessus servers that need to authenticate using SSL.

Nessus Client Keys

The Nessus user, which in this case is the user ID that Tenable.sc uses to communicate with the Nessus server, is created by the command `C:\Program Files\Tenable\Nessus\nessuscli mkcert-client`.

This command creates the keys for the Nessus clients and optionally registers them appropriately with the Nessus server by associating a distinguished name (dname) with the user ID. It is important



to respond **y** (yes) when prompted to register the user with the Nessus server for this to take effect. The user name may vary and is referred to here as **user**.

The certificate filename is a concatenation of **cert_**, the user name you entered and **.pem**. Additionally, the key filename is a concatenation of **key_**, the user name you entered and **.pem**.

The following files are created by this command:

File Name Created	Purpose
C:\Documents and Settings\<UserAccount>\Local Settings\Temp\nessus-xxxxxxx\cert_<user>.pem	This is the public certificate for the specified user.
C:\Documents and Settings\<UserAccount>\Local Settings\Temp\nessus-xxxxxxx\key_<user>.pem	This is the private key for the specified user.
C:\Program Files\Tenable\Nessus\nessus\users\<user_name>\auth\dname	This is the distinguished name to be associated with this user. The distinguished name consists of a number of options separated by commas in the following format: "/C={country}/ST={state}/L={location}/OU={organizational unit}/O={organization/CN={common name}"

Creating and Deploying SSL Authentication for Nessus

Create Keys and User on Nessus Server

To create the keys and user:

1. Create the Certificate Authority and Nessus server certificate using the command **C:\Program Files\Tenable\Nessus\nessuscli mkcert**



2. Provide the requested information.

Caution: Critical: Any Nessus Scanner that has previously processed scans will not initially accept these keys as a `policy.db` will have already been created on the Nessus Scanner. Remove the `policies.db` from the Nessus Scanner to ensure the deployment finishes successfully.

3. To remove the `policies.db` on a Linux system issue this command as root:

```
rm /opt/nessus/var/nessus/users/<UserName>/policies.db
```

4. To remove the `policies.db` on a Windows system, navigate to the `C:\Program Files\Tenable\Nessus` folder and remove the `policies.db` file. The actual location of the `policies.db` differs depending on the version of Windows that is running.

5. Create the user ID for the Nessus client, which is `Tenable.sc` in this case, to log in to the Nessus server with, key and certificate using the following command:

```
C:\Program Files\Tenable\Nessus\nessuscli mkcert-client
```

If the user does not exist in the Nessus user database, it is created. If it does exist, it is registered to the Nessus server and have a distinguished name (`dname`) associated with it. It is important to respond **y** (yes) when prompted to register the user with the Nessus server for this to take effect. The user must be a Nessus admin, so answer **y** when asked.

The certificates created contain the username entered previously, in this case **admin**, and are located in the directory as listed in the example above (e.g., `C:\Documents and Settings\<UserAccount>\Local Settings\Temp\nessus-00007fb1`). In the specified directory, the certificate and key files in this example are named `cert_admin.pem` and `key_admin.pem`.

Transfer Certificates and Keys to Tenable.sc

Transfer the `cert_admin.pem` and `key_admin.pem` files to a desired location on Tenable.sc, change into that directory and concatenate them as follows:

```
# cat cert_admin.pem key_admin.pem > nessuscert.pem
```

Note: The `nessuscert.pem` file will be used when configuring the Nessus scanner on Tenable.sc. This file needs to be copied to somewhere accessible for selection from your web browser during the Nessus configuration.

Configure Nessus Daemons



To enable certificate authentication on the Nessus server, the `force_pubkey_auth` setting must be enabled. Once enabled, log in to the Nessus server may only be completed by SSL certificates. Username and password login are disabled. As the root (or equivalent) user on the Nessus server, run the following command:

```
C:\Program Files\Tenable\Nessus\nessuscli fix --set force_pubkey_auth=yes
```

Open the Nessus Server Manager GUI, click **Stop Nessus Server** and then click **Start Nessus Server**.

Change the Nessus Mode of Authentication

In Tenable.sc, update your Nessus scanner configuration to use SSL certificate-based authentication. For more information, see [Add a Nessus Scanner](#).

Edit Nessus Scanner

General

Name*

Nessus Scanner

Description

Host*

nessus.example.com

Port*

8834

Enabled

☒

Verify Hostname

☐

Use Proxy

☐

Authentication

Type

SSL Certificate

Certificate*

nessuscert.pem



Offline Tenable.sc Plugin and Feed Updates

You can perform offline plugin updates and feed updates in air-gapped Tenable.sc environments.

- [Perform an Offline Nessus Plugin Update](#)
- [Perform an Offline NNM Plugin Update](#)
- [Perform an Offline Tenable.sc Feed Update](#)

Note: Tenable.sc does not manage plugins for LCE. However, LCE plugins are required for event analysis.

For general information about best practices in air-gapped environments, see [Considerations for Air-Gapped Environments](#).



Perform an Offline Nessus Plugin Update

Required User Role: Administrator

Before you begin:

- If you installed Tenable.sc in an environment other than Tenable Core, install a temporary Nessus scanner on the same host as Tenable.sc. You will use this temporary Nessus scanner to generate a challenge code for offline Tenable.sc registration. Do not start or otherwise configure the temporary Nessus scanner.

To perform an offline Nessus plugin update:

1. In the command line interface (CLI), run the following command to prevent the Nessus scanner from starting automatically upon restarting the system:

```
EL6 > /sbin/chkconfig nessusd off

EL7 > /usr/bin/systemctl disable nessusd
```

2. Run the following command and save the challenge string that is displayed:

```
# /opt/nessus/sbin/nessuscli fetch --challenge
```

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 Nessus installed. You cannot use the <https://plugins.nessus.org/v2/offline.php> page for Tenable.sc downloads.

4. Paste the challenge string from Step 3 and your Activation Code in the appropriate boxes on the web page.
5. Click **Submit**.



6. On the next page, copy the link that starts with **https://plugins.nessus.org/get.php...** and save it as a favorite. Within the saved link change **all-2.0.tar.gz** to **sc-plugins-diff.tar.gz**. This link will be needed for future use.

Caution: Do not click the link for nessus-fetch.rc.

7. Go to the favorite you created.

The page prompts you to download a file.

8. Download the file, which is called **sc-plugins-diff.tar.gz**.

9. Verify the file using the MD5 checksum, as described in the [knowledge base](#) article.

10. Save the **sc-plugins-diff.tar.gz** on the system used to access your Tenable.sc web interface.

11. Log in to Tenable.sc via the user interface.

12. Click **System > Configuration**.

The **Configuration** page appears.

13. Click **Plugins/Feed**.

The **Plugins/Feed Configuration** page appears.

14. In the **Schedules** section, expand the **Active Plugins** options.

15. Click **Choose File** and browse to the saved **sc-plugins-diff.tar.gz** file.

16. Click **Submit**.

After several minutes, the plugin update finishes and the page updates the **Last Updated** date and time.

What to do next:

- If you installed a temporary Nessus scanner on the same host as Tenable.sc, uninstall the Nessus scanner.



Perform an Offline NNM Plugin Update

Required User Role: Administrator

Before you begin:

- If you installed Tenable.sc in an environment other than Tenable Core, install a temporary Nessus scanner on the same host as Tenable.sc. You will use this temporary Nessus scanner to generate a challenge code for offline Tenable.sc registration. Do not start or otherwise configure the temporary Nessus scanner.

To perform an offline NNM plugin update:

1. In the command line interface (CLI), run the following command to prevent the NNM scanner from starting automatically upon restarting the system:

```
EL6 > /sbin/chkconfig nnm off

EL7 > /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 [NNM plugins page](#).
4. Paste the challenge string from Step 3 and your Activation Code in the appropriate boxes on the web page.
5. Click **Submit**.
6. On the next page, copy the link that starts with **https://plugins.nessus.org/v2/...** and bookmark it in your browser. The other information on the page is not relevant for use with Tenable.sc.
7. Click the bookmarked link.



The page prompts you to download a file.

8. Download the file, which is called `sc-passive.tar.gz`.
9. Verify the file using the MD5 checksum, as described in the [knowledge base](#) article.
10. Save the `sc-passive.tar.gz` on the system used to access your Tenable.sc GUI.

Note: Access the NNM feed setting and change the activation from offline to Tenable.sc.

11. Log in to Tenable.sc 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 Nessus scanner on the same host as Tenable.sc, uninstall the Nessus scanner.



Perform an Offline Tenable.sc Feed Update

Required User Role: Administrator

Note: If you already performed a Nessus offline plugin update, start at step 7.

Before you begin:

- If you installed Tenable.sc in an environment other than Tenable Core, install a temporary Nessus scanner on the same host as Tenable.sc. You will use this temporary Nessus scanner to generate a challenge code for offline Tenable.sc registration. Do not start or otherwise configure the temporary Nessus scanner.

To perform an offline Tenable.sc feed update:

1. In the command line interface (CLI), run the following command to prevent the Nessus scanner from starting automatically upon restarting the system:

```
EL6 >
/sbin/chkconfig nessusd off

EL7 >
/usr/bin/systemctl disable nessusd
```

2. To obtain the challenge code for an offline Tenable.sc registration, do one of the following:

- If you deployed Tenable.sc + Tenable Core, navigate to the **Tenable.sc** tab in Tenable Core and save the challenge code.
- If you installed Tenable.sc 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 MD5 checksum, as described in the [knowledge base](#) article.
11. Save the **SecurityCenterFeed48.tar.gz** on the system used to access your Tenable.sc GUI.
12. Log in to Tenable.sc via the user interface.
13. Click **System > Configuration**.

The **Configuration** page appears.

14. Click **Plugins/Feed**.

The **Plugins/Feed Configuration** page appears.

15. In the **Schedules** section, expand the **Tenable.sc Feed** options.
16. Click **Choose File** and browse to the saved **SecurityCenterFeed48.tar.gz** file.
17. Click **Submit**.

After several minutes, the plugin update finishes and the page updates the **Last Updated** date and time.

What to do next:



- If you installed a temporary Nessus scanner on the same host as Tenable.sc, uninstall the Nessus scanner.



Troubleshooting

This troubleshooting section covers some of the common issues encountered with Tenable.sc.

- [General Tenable.sc Troubleshooting](#)
- [LCE Troubleshooting](#)
- [Nessus Troubleshooting](#)
- [NNM Troubleshooting](#)
- [Troubleshooting Issues with the custom_CA.inc File](#)



General Tenable.sc Troubleshooting

Tenable.sc does not appear to be operational

1. If a login page does not appear, close and reopen the web browser.
2. Ensure that the remote httpd service is running on the Tenable.sc host:

```
# ps ax | grep httpd
1990 ?          Ss      0:01 /opt/sc/support/bin/httpd -k start
```

3. Ensure that sufficient drive space exists on the Tenable.sc host:

```
# df

Filesystem                1K-
blocks      Used        Available      Use%      Mounted on
/dev/mapper/VolGroup00-LogVol00
8506784      0            100%      /
/dev/sda1
101086       24455        71412      26%
/boot
tmpfs
1037732      0%           /dev/shm    1037732      0
```

4. If there is not enough drive space, recover sufficient space and restart the Tenable.sc 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.sc 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.



LCE Troubleshooting

LCE server does not appear to be operational

1. Confirm that the LCE server state is **Working** along with all attached LCE clients.
2. Check that you can SSH from the Tenable.sc host to the LCE host.
3. Check that the LCE daemon is running on its host and listening on the configured port (TCP port 31300 by default):

```
# ss -pan | grep lced
```

```
tcp          0      0 0.0.0.0:31300 0.0.0.0:*    LISTEN      30339/lced
```

4. Check that the listening ports can be reached from the network and are not blocked by a fire-wall.
5. If the LCE server is not operational, attempt to start the service:

```
# service lce start
```

```
Starting Log Correlation EngineLCE Daemon Configuration
```

```
LICENSE: Tenable Log Correlation Engine 3-Silo Key for [user]
```

```
EXPIRE: 11-10-2011
```

```
REMAIN: 30 days
```

```
MESSAGE: LCE (3-silo license)
```

```
MESSAGE: Valid authorization
```

```
-----
```

```
[ OK ]
```

No events from an attached LCE server

1. Confirm that the LCE server state is **Working** along with all attached LCE clients.
2. Confirm connectivity by checking that heartbeat events show up in the Tenable.sc UI.
3. Check the LCE configuration settings in accordance with the LCE documentation.



4. Check the individual LCE client configuration and authorization. If syslog is being used to collect information and events, ensure that the syslog service is running and configured correctly on the target syslog server in accordance with LCE documentation.
5. Check for NTP time synchronization between the Tenable.sc, LCE, and LCE clients.

Invalid LCE license

1. Check that an up-to-date license exists on the LCE server.

LCE plugins fail to update

1. Manually test a plugin update under **Plugins** with **Update Plugins**. If successful, the line **Passive Plugins Last Updated** will update to the current date and time.
2. Ensure that the Tenable.sc host is allowed outbound HTTPS connectivity to the LCE Plugin Update Site.
3. For all other LCE plugin update issues, contact Tenable Support.



Nessus Troubleshooting

Nessus server does not appear to be operational

1. Verify that the Nessus scanner **Status** is **Unable to Connect**.
2. SSH to the remote Nessus host to make sure the underlying operating system is operational.
3. Confirm that the Nessus daemon is running (Linux example below):

```
# service nessusd status
nessusd (pid 3853) is running...
```

4. If the Nessus service is not running, start the service:

```
# service nessusd start
Starting Nessus services:
# ps -ef | grep nessusd
root      8201   8200  60 11:41 pts/2    00:00:05 nessusd -q
root      8206   7842   0 11:41 pts/2    00:00:00 grep nessusd
#
```

Cannot add a Nessus server

1. Make sure the Nessus daemon was registered using the Tenable.sc option for registration.
2. Check connectivity from Tenable.sc to the port the Nessus system is running on (e.g., 8834).
For example, run:

```
curl -k https://<scannerIPAddress>:<port>
```

Nessus scans fail to complete

1. Ensure that the Nessus service is running on the Nessus host.
2. Ensure that Nessus scanner is listed in Tenable.sc under **Resources > Nessus Scanners** and that the status of the Nessus scanner is listed as **Working**. For more information, see [Nessus Scanner Statuses](#).



3. Click **Edit** to ensure that the IP address or hostname, port, username, password, and selected repositories for the Nessus scanner are all correct.
4. Edit any incorrect entries to their correct state.
5. Click **Submit** to attempt to reinitialize the Nessus scanning interface.
6. Right click the scan results and click **Scan Details** to obtain a more detailed description of the error.

If the scan details indicate a Blocking error, this is indicative of a license IP address count that has reached the limit. Either remove a repository to free up IP addresses or obtain a license for more IP addresses.

7. Ensure that scan targets are permitted within the configured scan zones.
8. Ensure the Nessus scanner is running a supported Nessus version. For minimum Nessus scanner version requirements, see the [Tenable.sc Release Notes](#) for your version.

Nessus plugins fail to update

1. Click **System > Configuration**.

The **Configuration** page appears.

2. Click **License** and ensure that the Nessus Activation Code is marked as **Valid**.
3. Ensure the Nessus scanner is running a supported Nessus version. For minimum Nessus scanner version requirements, see the [Tenable.sc Release Notes](#) for your version.
4. Ensure that the user used to connect to the Nessus server is a Nessus administrator.
5. Ensure that the Tenable.sc system is allowed outbound HTTPS connectivity to the Nessus Plugin Update Site.
6. Under **System, Configuration**, and **Update** in Tenable.sc, ensure that Active Plugins is not set to **Never**.
7. Manually test a plugin update under **Plugins** with **Update Plugins**.

If successful, the line **Active Plugins Last Updated** updates to the current date and time.

8. For all other Nessus plugin update issues, contact Tenable Support.



NNM Troubleshooting

NNM server does not appear to be operational

1. Verify that the NNM server appears as **Unable to Connect** under **Status**.
2. SSH to the remote NNM host to make sure the underlying operating system is operational.
3. Confirm that the NNM is running (Linux example below):

```
# service pvs status

NNM is stopped
NNM Proxy (pid 3142) is running
#
```

4. If the NNM service is not running, start the service:

```
# service nnm start
Starting NNM Proxy           [ OK ]
Starting NNM                 [ OK ]
#
```

Cannot add a NNM server

1. Confirm that the NNM proxy is listening on the same port as Tenable.sc (port 8835 by default):

```
# ss -pan | grep 8835
tcp        0      0 0.0.0.0:8835      0.0.0.0:*        LISTEN     406/pvs
```

2. Check connectivity by telnetting from the Tenable.sc console into the NNM server on port 8835 (the NNM listening port). If successful, the response includes: Escape character is '^'.

No vulnerabilities are being received from the NNM server



1. Ensure that the NNM service is running on the NNM host.
2. Ensure that the NNM appears in Tenable.sc under **Resources > Nessus Network Monitors** and that the status of the NNM appears as **Working**.
3. Click **Edit** to ensure that the IP address or hostname, port, username, password, and selected repositories for the NNM are correct.
4. Edit any incorrect entries to their correct state.
5. Click **Submit** to attempt to reinitialize the NNM scanning interface.

NNM plugins fail to update

1. Manually test a plugin update under **Plugins** with **Update Plugins**.
If successful, **Passive Plugins Last Updated** updates to the current date and time.
2. Ensure that the Tenable.sc host allows outbound HTTPS connectivity to the NNM Plugin Update Site.
3. For all other NNM plugin update issues, contact Tenable Support.