



Tenable Nessus Network Monitor 6.1.x User Guide

Last Updated: July 05, 2023



Table of Contents

Welcome to Tenable Nessus Network Monitor	8
Get Started with Tenable Nessus Network Monitor	9
Tenable Nessus Network Monitor Navigation	11
View Tenable Nessus Network Monitor Information	13
System Requirements	14
Tenable Nessus Network Monitor Hardware Requirements	15
Tenable Nessus Network Monitor Software Requirements	17
Tenable Nessus Network Monitor Licensing Requirements	20
Download Tenable Nessus Network Monitor	21
Install Tenable Nessus Network Monitor	22
Upgrade Tenable Nessus Network Monitor	33
Upgrade Tenable Nessus Network Monitor on Linux	34
Upgrade Tenable Nessus Network Monitor on Windows	35
Upgrade Tenable Nessus Network Monitor on macOS	36
Set up Tenable Nessus Network Monitor	37
Configure Tenable Nessus Network Monitor	38
Verify Your RPM Signature	41
Register Tenable Nessus Network Monitor Offline via the Tenable Nessus Network Monitor Interface	42
Register Tenable Nessus Network Monitor Offline via the CLI	44
Register High Performance Mode Tenable Nessus Network Monitor for Tenable Security Center in an Air-gapped Environment	46
Disable Secure Boot for Tenable Nessus Network Monitor High Performance Mode	49



Configure High Performance Mode	51
Configure Tenable Nessus Network Monitor in High Performance Mode on Hyper-V	53
Configure Hyper-V NIC in Promiscuous Mode	59
Configure Tenable Nessus Network Monitor on Machines Hosting Napatech Acceleration Cards	60
Troubleshoot Issues with Napatech in Tenable Nessus Network Monitor	62
Remove Tenable Nessus Network Monitor	64
Remove Tenable Nessus Network Monitor from Linux	65
Remove Tenable Nessus Network Monitor from Windows	66
Remove Tenable Nessus Network Monitor from macOS	67
Monitoring Page	68
Dashboards Section	72
Rearrange Charts	75
Refresh a Chart	76
Set a Date Range for the Dashboards Section	77
Remove a Chart from a Dashboard	78
Hosts Section	79
Vulnerabilities Section	84
Delete a Vulnerability	85
SIEM Analysis Section	86
Applications Section	89
Operating Systems Section	90
Connections Section	91
Mobile Devices Section	92
Filter Monitoring Results	93



Export Monitoring Results	94
Launch a Tenable Nessus Scan	95
Results Page	96
Upload a Report	97
Upload a Pcap	98
Filter Results	99
Delete Results	100
Users Page	101
Create a New User	102
Modify a User Account	104
Reset a Locked Account	105
Delete a User	106
Configuration Page	107
Tenable Nessus Network Monitor Settings Section	108
Configure Tenable Nessus Network Monitor Performance Mode	124
Feed Settings Section	126
Download New Vulnerability Plugins	128
Updating the Tenable Nessus Network Monitor Management Interface	129
Cloud Settings Section	130
Industrial Security Settings Section	132
Web Proxy Settings Section	134
Chart Settings Section	136
Create a Custom Chart	137
Delete a Chart	139



Email Settings Section	140
Create an Email Notification	142
Delete an Email Notification	144
Plugin Settings Section	145
Add a Plugin Field	149
Delete a Custom Plugin	150
Nessus Scanner Settings Section	151
Add a Tenable Nessus Scanner	152
Delete a Tenable Nessus Scanner	153
Additional Resources	154
Command Line Operations	155
Common Command Line Operations	156
Linux Command Line Operations	161
Windows Command Line Operations	166
macOS Command Line Operations	169
Configure Tenable Nessus Network Monitor for Certificates	171
Create a Custom CA and Server Certificate	172
Create Tenable Nessus Network Monitor SSL Certificates for Login	174
Connect to Tenable Nessus Network Monitor with a User Certificate	176
Custom SSL Certificates	177
Configure Tenable Nessus Network Monitor for NIAP Compliance	179
Encryption Strength	183
File and Process Allow List	185
Modules	187



Connection Analysis Module	188
Tenable Nessus Network Monitor Plugins	192
About Tenable Nessus Network Monitor Plugins	193
Tenable Nessus Network Monitor Fingerprinting	194
Tenable Nessus Network Monitor Plugin Syntax	195
Network Client Detection	200
Pattern Matching	201
Time Dependent Plugins	204
Plugin Examples	206
Tenable Nessus Network Monitor Real-Time Plugin Syntax	209
Real-Time Plugin Examples	211
Tenable Nessus Network Monitor Corporate Policy Plugins	215
Detecting Custom Activity Prohibited by Policy	216
Detecting Confidential Data in Motion	219
Internal Tenable Nessus Network Monitor Plugin IDs	221
Real-Time Traffic Analysis Configuration Theory	224
Focus Network	225
Detecting Server and Client Ports	226
Detecting Specific Server and Client Port Usage	227
Firewall Rules	229
Working with Tenable Security Center	230
Selecting Rule Libraries and Filtering Rules	231
Detecting Encrypted and Interactive Sessions	232
Routes and Hop Distance	233



Alerting	234
Syslog Messages	235
Standard Syslog Message Types	236
CEF Syslog Message Types	238
Unknown or Customized Ports	239
Working with Tenable Security Center	240
Managing Vulnerabilities	241
Offline Tenable Nessus Network Monitor Plugin Update in Tenable Security Center	242
Tenable Security Center Troubleshooting	244



Welcome to Tenable Nessus Network Monitor

This user guide describes the Tenable Nessus Network Monitor® (formerly known as NNM) 6.1.x (Patent 7,761,918 B2) architecture, installation, operation, and integration with Tenable Security Center and Tenable Vulnerability Management, and export of data to third parties. For assistance, contact Tenable Support.

Tip: If you are new to Tenable Nessus Network Monitor, see the [Workflow](#).

Passive vulnerability scanning is the process of monitoring network traffic at the packet layer to determine topology, clients, applications, and related security issues. Tenable Nessus Network Monitor also profiles traffic and detects compromised systems.

Tenable Nessus Network Monitor can:

- Detect when systems are compromised with application intrusion detection.
- Highlight all interactive and encrypted network sessions.
- Detect when new hosts are added to a network.
- Track which systems are communicating on which ports.
- Detect which ports are served and which are browsed by each system.
- Detect the number of hops to each monitored host.

Note: For security purposes, Tenable® does not recommend configuring Tenable Nessus Network Monitor as internet facing software.



Get Started with Tenable Nessus Network Monitor

1. Ensure that your setup meets the minimum system requirements:
 - [Hardware requirements](#)
 - [Software requirements](#)
2. Obtain the proper [license or Activation Code for Tenable Nessus Network Monitor](#) for your configuration.

Note: See special activation code instructions for integration with Tenable Security Center or Tenable Vulnerability Management.

3. Follow the installation steps for your environment:
 - [Linux](#)
 - [Windows](#)
 - [macOS](#)
 - [Tenable Core](#)
4. (Optional) [Configure Virtual Switches for use with Tenable Nessus Network Monitor.](#)
5. Perform the [initial configuration steps](#) for Tenable Nessus Network Monitor in the web interface.

After configuration, Tenable Nessus Network Monitor begins monitoring incoming traffic immediately.

Note: If you wish to [register Tenable Nessus Network Monitor offline](#) or run Tenable Nessus Network Monitor in [High Performance mode](#), you must follow several additional configuration steps.

6. [Create users in Tenable Nessus Network Monitor](#) and set [administrative privileges](#) as necessary.
7. You can view monitored traffic results in dashboards on the [Monitoring page](#) and historical data in snapshots and reports on the [Results page](#).



Note: By default, Tenable Nessus Network Monitor has discovery mode enabled when installed. You must disable discovery mode for Tenable Nessus Network Monitor to load plugins into memory. For more information on discovery mode, see [Tenable Nessus Network Monitor Settings Section](#).

For more Tenable Nessus Network Monitor deployment information, see the [Tenable Nessus Network Monitor Deployment Guide](#).



Tenable Nessus Network Monitor Navigation

The top navigation menu displays two main pages: **Monitoring** and **Results**. All of Tenable Nessus Network Monitor's primary analysis tasks can be performed using these two pages. Click a page name to open that page.



From the right side of the top navigation menu, you can access settings (⚙️), current user settings (username of the currently logged-in user), and notifications (🔔).

- Click the ⚙️ icon to display the [Users](#) and [Configuration](#) options, where you can make administrative changes to Tenable Nessus Network Monitor.

Note: The **Users** and **Configuration** pages are available only to users with administrative privileges.

- Click your username to display a drop-down box with the following options:
 - **Change Password** - Change password for the current user.
 - **Help & Support** - [View Tenable Nessus Network Monitor Information](#) and documentation.
 - **Sign Out** - Log out as the current user.
- The bell (🔔) icon toggles the **Notification History** box, which displays a list of notifications, successful or unsuccessful login attempts, errors, and system information generated by Tenable Nessus Network Monitor. The color of the bell changes based on the nature of the notifications in the list. If there are no alerts, or all notifications are information alerts, then the bell is blue (🔔). If there are error alerts in the notification list, then the bell is red (🔴). The **Notification History** box displays up to 1,000 alerts. Once the limit is reached, no new alerts can be listed until old ones are cleared.




NOTIFICATION HISTORY **COUNT: 2**

ERROR **October 24, 2017 11:50:29** ✕
Failed to update email settings Error: SMTP
From Address was not specified

INFO **October 24, 2017 11:29:12** ✕
Password for admin changed successfully.

Close Clear History

To remove notifications individually, click the  button to the right of the description of each event. Alternatively, click the **Clear History** button in the bottom right corner of the box to delete the entire notification history.

Note: Notifications are not preserved between sessions. Unread notifications are removed from the list when the user logs out.



View Tenable Nessus Network Monitor Information

You can view information about your instance of Tenable Nessus Network Monitor such as the version number, web server version, HTML client version, license information, feed ID, the feed expiration date, and performance mode.

To view information about your instance of Tenable Nessus Network Monitor:

- In the top navigation bar, click your username > **Help & Support**.

View information for your instance of Tenable Nessus Network Monitor.



System Requirements

This section describes the following system requirements for Tenable Nessus Network Monitor:

- [Tenable Nessus Network Monitor Hardware Requirements](#)
- [Tenable Nessus Network Monitor Software Requirements](#)
- [Tenable Nessus Network Monitor Licensing Requirements](#)



Tenable Nessus Network Monitor Hardware Requirements

Enterprise networks can vary in performance, capacity, protocols, and overall activity. Resource requirements to consider for Tenable Nessus Network Monitor deployments include raw network speed, the size of the network being monitored, and the configuration of Tenable Nessus Network Monitor.

The following chart outlines some basic hardware requirements for operating Tenable Nessus Network Monitor:

Version	Installation scenario	RAM	Processor	Hard Disk
All Versions	Tenable Nessus Network Monitor managing up to 50,000 hosts * (**)	2 GB RAM (4 GB RAM recommended)	2 2GHz cores	20 GB HDD minimum
	Tenable Nessus Network Monitor managing more than 50,000 hosts **	4 GB RAM (8 GB RAM recommended)	4 2GHz cores	20 GB HDD minimum
	Tenable Nessus Network Monitor running in High Performance mode	16 GB RAM (HugePages memory: 2 GB)	10 2GHz cores with hyper-threading enabled	20 GB HDD minimum

*The ability to monitor a given number of hosts depends on the bandwidth, memory, and processing power available to the system running Tenable Nessus Network Monitor.

**For optimal data collection, Tenable Nessus Network Monitor must be connected to the network segment via a hub, spanned port, or network tap to have a full, continuous view of network traffic.



Note: Research your VM software vendor for comparative recommendations, as VMs typically see up to a 30% loss in efficiency compared to dedicated servers. Tenable Nessus Network Monitor supports VMware's vmxnet3 driver.

High Performance Mode

To run Tenable Nessus Network Monitor in High Performance mode, a minimum of two of the following types of Intel NICs are required; one as a management interface and at least one as a monitoring interface:

- e1000 (82540, 82545, 82546)
- e1000e (82571, 82574, 82583, ICH8.ICH10, PCH.PCH2)
- igb (82575, 82576, 82580, I210, I211, I350, I354, DH89xx)
- ixgbe (82598, 82599, X540, X550)
- i40e (X710, XL710)
- NT40A01-4x1



Tenable Nessus Network Monitor Software Requirements

Note: Standard support for Tenable Nessus Network Monitor 5.12 ends 09/30/2022. Tenable recommends updating to Tenable Nessus Network Monitor 6.0.0 or later. Otherwise, you will not be able to report issues and bugs. Users that connect to Tenable Vulnerability Management using a web proxy need to upgrade to Tenable Nessus Network Monitor 6.1.1.

Tenable Nessus Network Monitor is available for the following platforms:

Version	Software Requirements
6.2.x	<ul style="list-style-type: none">• Red Hat Linux ES 7 / CentOS 7 (through 7.9) 64-bit• Red Hat Linux ES 8 / CentOS 8 (through 8.7) 64-bit• Red Hat Linux ES 9 64-bit <p>Note: For all versions of Red Hat Linux ES and CentOS, Tenable Nessus Network Monitor requires that you have <code>systemd</code> and <code>firewalld</code> on your system.</p> <ul style="list-style-type: none">• Microsoft Windows 7, 8, 10, Server 2012, Server 2016, and Server 2019 64-bit <p>Note: Tenable Nessus Network Monitor requires Microsoft Visual C++ Redistributable for Visual Studio 2015, 2017 and 2019. You must download the specific package <code>vc_redist.x64.exe</code> from the Microsoft downloads site.</p> <p>High Performance mode only available on:</p> <ul style="list-style-type: none">• RH7/CentOS7 (RH 7.0 through RH 7.9) : 3.10.0-1160• RH8/CentOS8 (RH 8.0 through 8.5): 4.18.0-348• RH8 (RH 8.6-8.7): 4.18.0-425
6.1.x	<ul style="list-style-type: none">• Red Hat Linux ES 7 / CentOS 7 (through 7.9) 64-bit <p>Note: For this version, Tenable Nessus Network Monitor requires that you have <code>systemd</code> and <code>firewalld</code> on your system.</p> <ul style="list-style-type: none">• Red Hat Linux ES 8 / CentOS 8 (through 8.5) 64-bit



Note: For this version, Tenable Nessus Network Monitor requires that you have `systemd` and `firewalld` on your system.

- Microsoft Windows 7, 8, 10, Server 2008, Server 2012, Server 2016, and Server 2019 64-bit

Note: Tenable Nessus Network Monitor requires Microsoft Visual C++ Redistributable for Visual Studio 2015, 2017 and 2019. You must download the specific package `vc_redist.x64.exe` from the [Microsoft downloads site](#).

High Performance mode only available on:

- RH7/CentOS7 (RH 7.0 through RH7.4) : 3.10.0-693
- RH7/CentOS7 (RH 7.5): 3.10.0-862
- RH7/CentOS7 (RH 7.6): 3.10.0-957
- RH7/CentOS7 (RH 7.7): 3.10.0-1062
- RH7/CentOS7 (RH 7.8): 3.10.0-1127
- RH7/CentOS7 (RH 7.9): 3.10-1160
- RH8/CentOS8 (RH 8.0 through 8.5): 4.18.0-348

You can use ERSPAN to mirror traffic from one or more source ports on a virtual switch, physical switch, or router and send the traffic to a destination IP host running Tenable Nessus Network Monitor. Tenable Nessus Network Monitor supports the following ERSPAN virtual environments:

- VMware ERSPAN (Transparent Ethernet Bridging)
- Cisco ERSPAN (ERSPAN Type II)

Tip: Refer to the [Configuring Virtual Switches for Use with Tenable Nessus Network Monitor](#) document for details on configuring your virtual environment.

High Performance Mode

To run Tenable Nessus Network Monitor in High Performance mode, you must enable HugePages support. HugePages is a performance feature of the Linux kernel and is necessary for the large memory pool allocation used for packet buffers. If your Linux kernel does not have HugePages



configured, Tenable Nessus Network Monitor automatically configures HugePages per the appropriate settings. Otherwise, if your Linux kernel has defined HugePages, refer to the Configuring HugePages instructions in the [Linux Command Line Operations](#) section.



Tenable Nessus Network Monitor Licensing Requirements

Tenable Nessus Network Monitor Subscription

An Tenable Nessus Network Monitor subscription Activation Code is available that enables Tenable Nessus Network Monitor to operate in Standalone mode. Use this mode to view results from an HTML interface enabled on the Tenable Nessus Network Monitor server.

Activation Code

To obtain a Trial Activation Code for Tenable Nessus Network Monitor, contact sales@tenable.com. Trial Activation Codes are handled the same way by Tenable Nessus Network Monitor as full Activation Codes, except that Trial Activation Codes allow monitoring for only 30 days. During a trial of Tenable Nessus Network Monitor, all features are available.

Tenable Security Center Continuous View

Tenable Security Center CV includes Tenable Nessus Network Monitor as part of a bundled license package with Tenable Security Center. This license allows an unlimited number of Tenable Nessus Network Monitor deployments to monitor an unlimited number of networks. Tenable Security Center CV's IP view is constrained by the license with which it is purchased.

Tenable Vulnerability Management

Tenable Vulnerability Management includes Tenable Nessus Network Monitor as part of a bundled license package with Tenable Vulnerability Management. This license allows an unlimited number of Tenable Nessus Network Monitor deployments to monitor an unlimited number of networks. Tenable Vulnerability Management's Asset view is constrained by the license with which it is purchased.

High Performance Mode

Tenable Nessus Network Monitor in High Performance Mode can be licensed in Standalone mode or bundled with Tenable Security Center.



Download Tenable Nessus Network Monitor

To download Tenable Nessus Network Monitor:

1. Access the [Tenable Downloads](#) page.
2. Click **Tenable Nessus Network Monitor**.
3. Select the correct version for your operating system.

After you accept the license agreement, a download begins.

Note: To ensure binary compatibility, be sure to download the correct build for your operating environment.

4. Confirm the integrity of the installation package by comparing the download checksum with the checksum on the [Tenable downloads](#) page, as described in the [knowledge base](#) article.



Install Tenable Nessus Network Monitor

Before You Begin

- [Download](#) the Tenable Nessus Network Monitor package.
- Ensure you can run the following commands with administrative or root privileges.

Linux

To ensure audit record time stamp consistency between Tenable Nessus Network Monitor and Tenable Security Center, ensure the underlying OS makes use of NTP as described in the [Red Hat documentation](#).

The [software license agreement](#) for Tenable Nessus Network Monitor is located in the `/opt/nnm/docs` directory.

Tip: Ensure that organizational and OS firewall rules permit access to port 8835 on the Tenable Nessus Network Monitor server.

To install Tenable Nessus Network Monitor on Linux:

1. Install the Tenable Nessus Network Monitor `.rpm` file downloaded from the [Tenable Downloads](#) page in RedHat or CentOS with the following command. The specific filename varies depending on your platform and version.

```
# dnf install Tenable Nessus Network Monitor-5.x.x-esx.x86_64.rpm
Preparing...      ##### [100%]
1:NNM             ##### [100%]
[*] Tenable Nessus Network Monitor installation completed.
#
```

The installation creates the `/opt/nnm` directory, which contains the Tenable Nessus Network Monitor software, default plugins, and directory structure.

2. (Optional) You can verify the rpm's signature before deploying. See [Verify the RPM Signature](#).
3. Start Tenable Nessus Network Monitor for Red Hat and CentOS systems using the following command:

```
# service nnm start
```



4. Navigate to **https://<IP address or hostname>:8835**, which displays the Tenable Nessus Network Monitor web front end to log in for the first time.

Refer to [Configure Tenable Nessus Network Monitor](#) to complete the initial login.

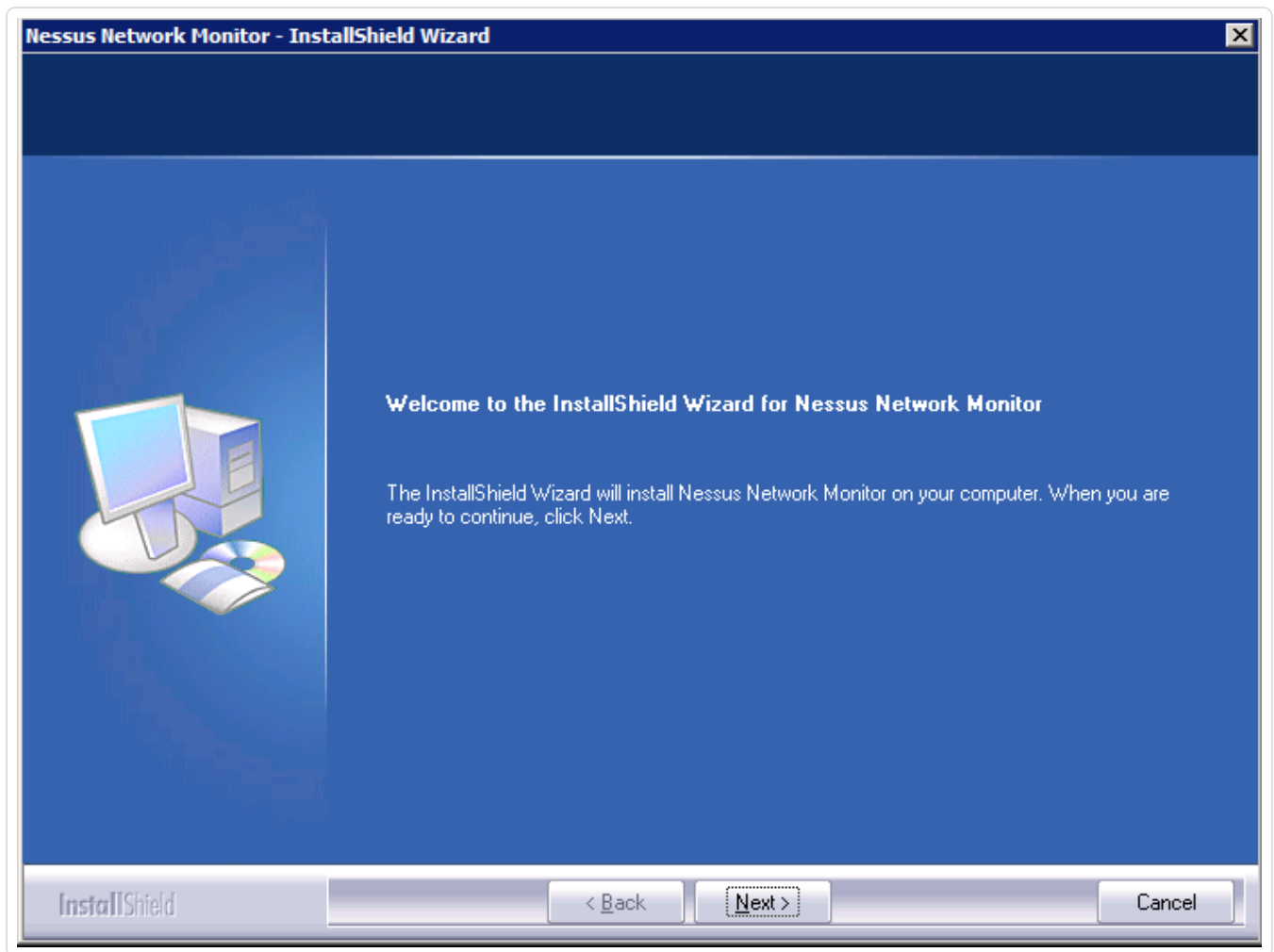
Windows

You must ensure the latest version of Microsoft Visual C++ 2010 Redistributable Package is installed for your 64-bit platform and architecture. Be sure to stop any other programs on your system that utilize WinPcap.

To install Tenable Nessus Network Monitor on Windows:

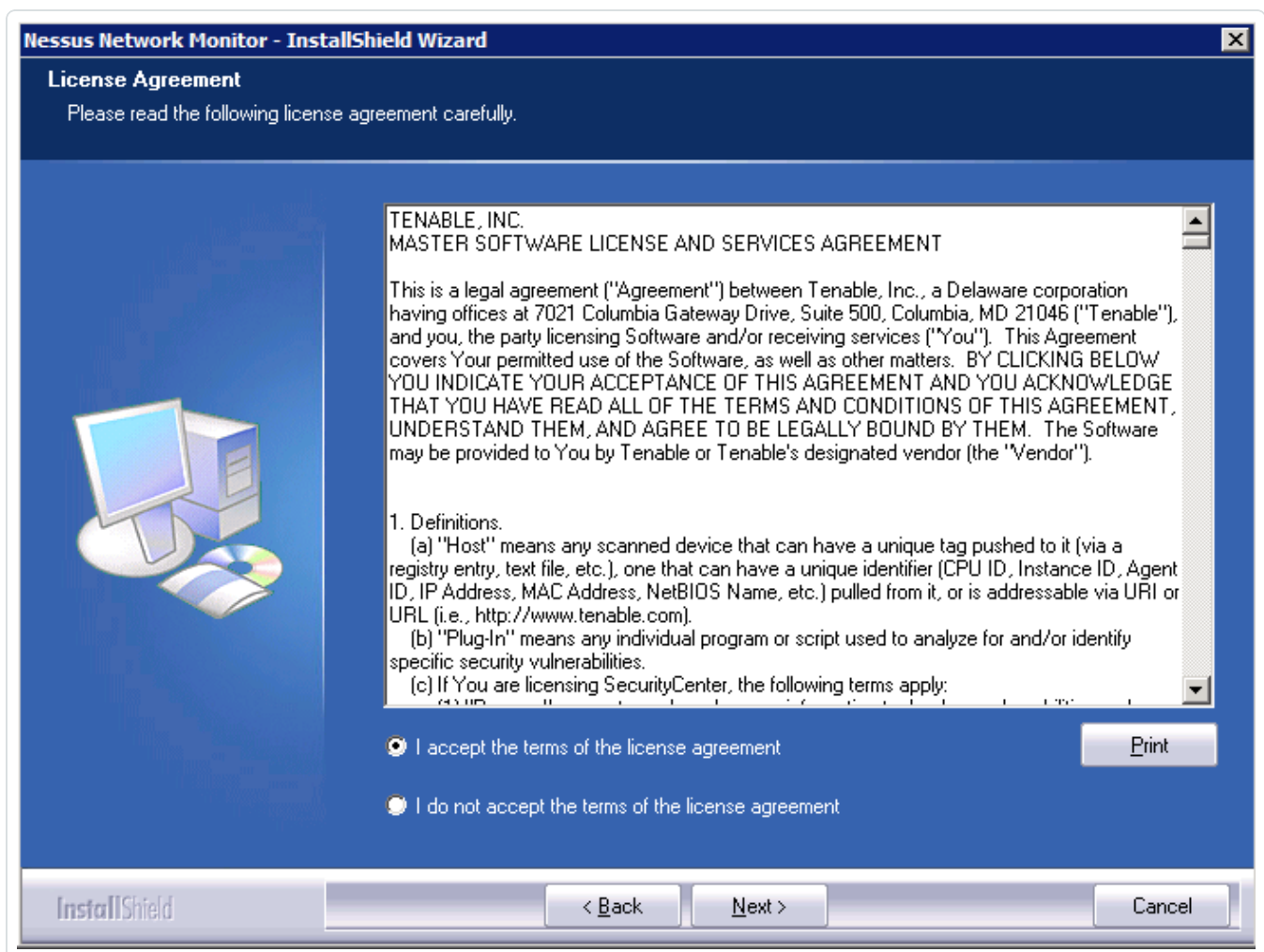
1. Double-click the **.exe** file downloaded from the [Tenable Downloads](#) page. The specific file-name varies depending on your version.

The InstallShield Wizard launches, which walks you through the installation process and required configuration steps.



2. Click the **Next** button.

The **License Agreement** screen appears.

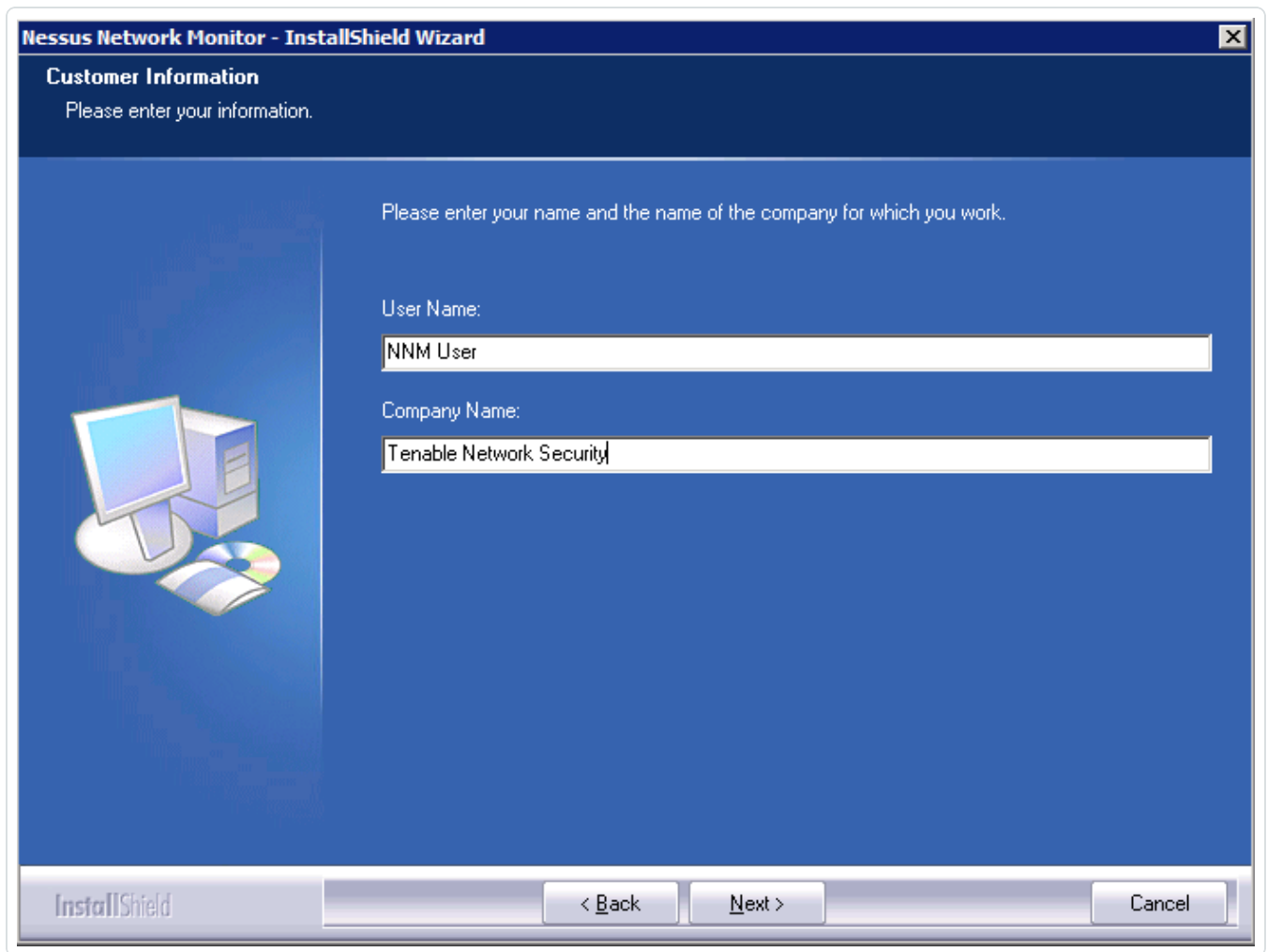


3. Agree to the terms to continue the installation process and use Tenable Nessus Network Monitor.

Tip: You can copy the text of the agreement into a separate document for reference, or you can click the **Print** button to print the agreement directly from this screen.

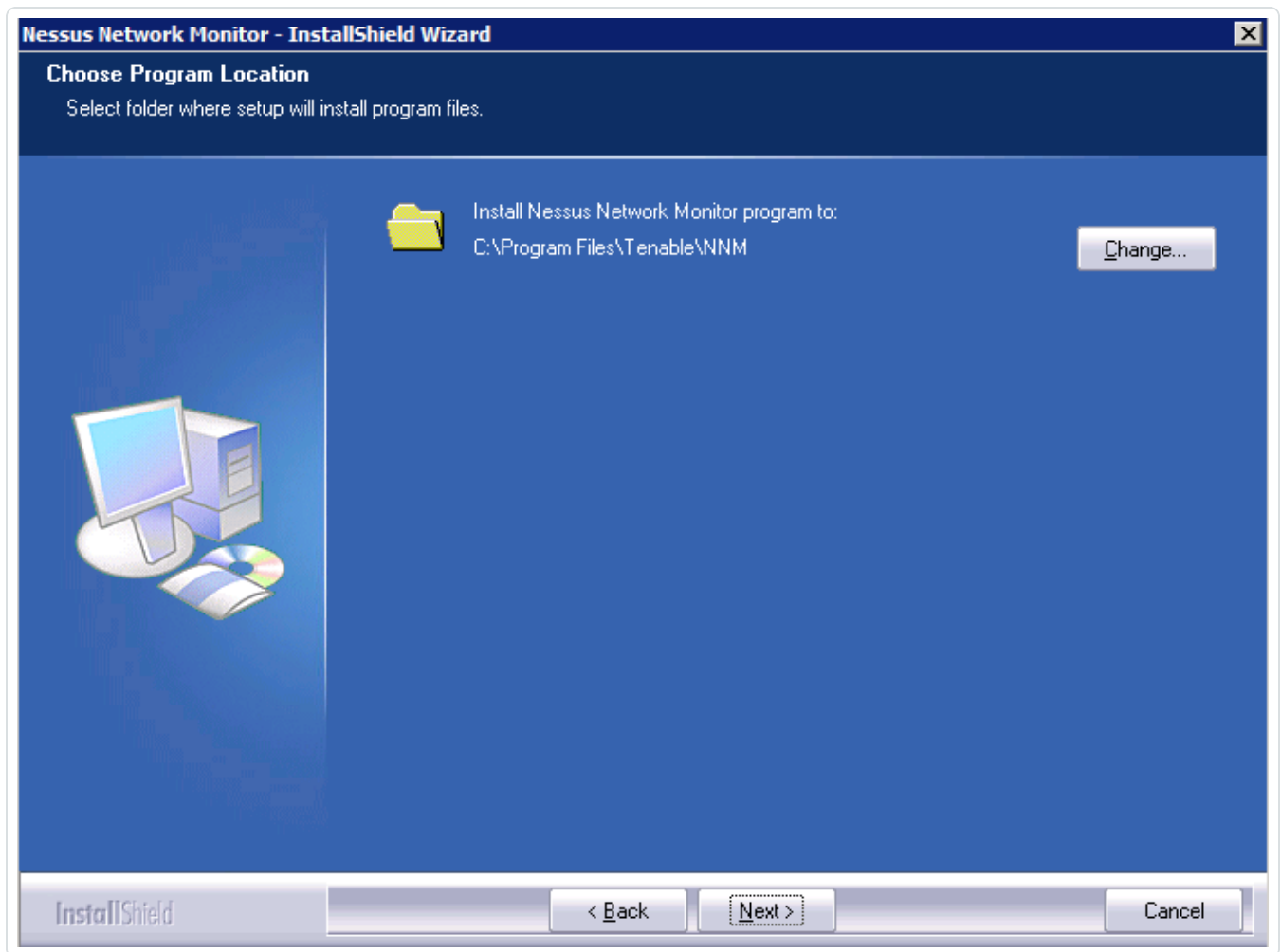
4. Click the **Next** button.

The **Customer Information** screen appears. The **User Name** and **Company Name** boxes are used to customize the installation, but are not related to any configuration options (e.g., for interfacing with Tenable Security Center).



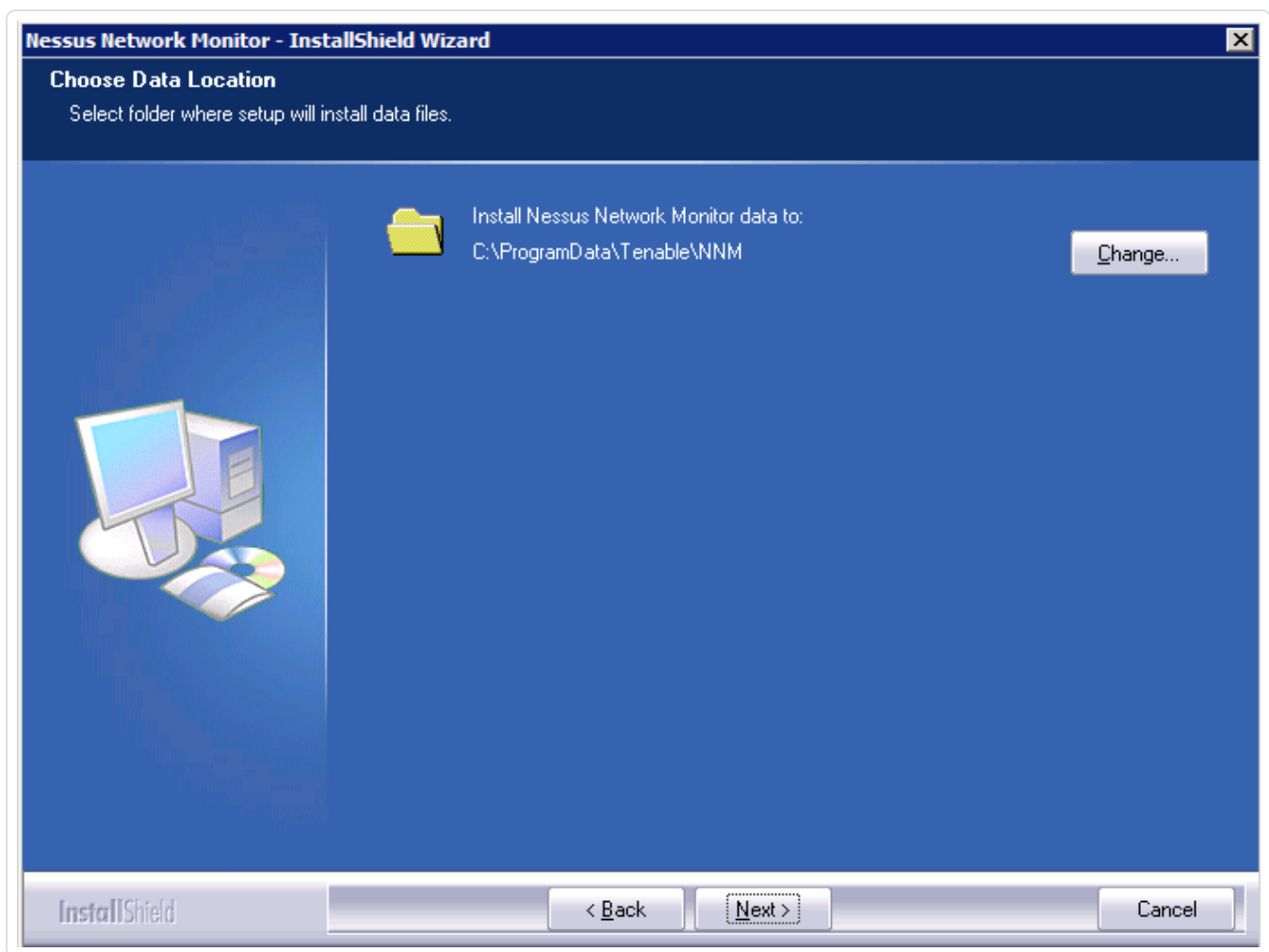
5. Click the **Next** button.

The **Choose Program Location** screen appears, where you can verify the location in which the Tenable Nessus Network Monitor binaries are installed.



6. Click the **Change** button to specify a custom path.
7. Click the **Next** button.

The **Choose Data Location** screen appears, where you can verify the location in which user data generated by Tenable Nessus Network Monitor is stored.

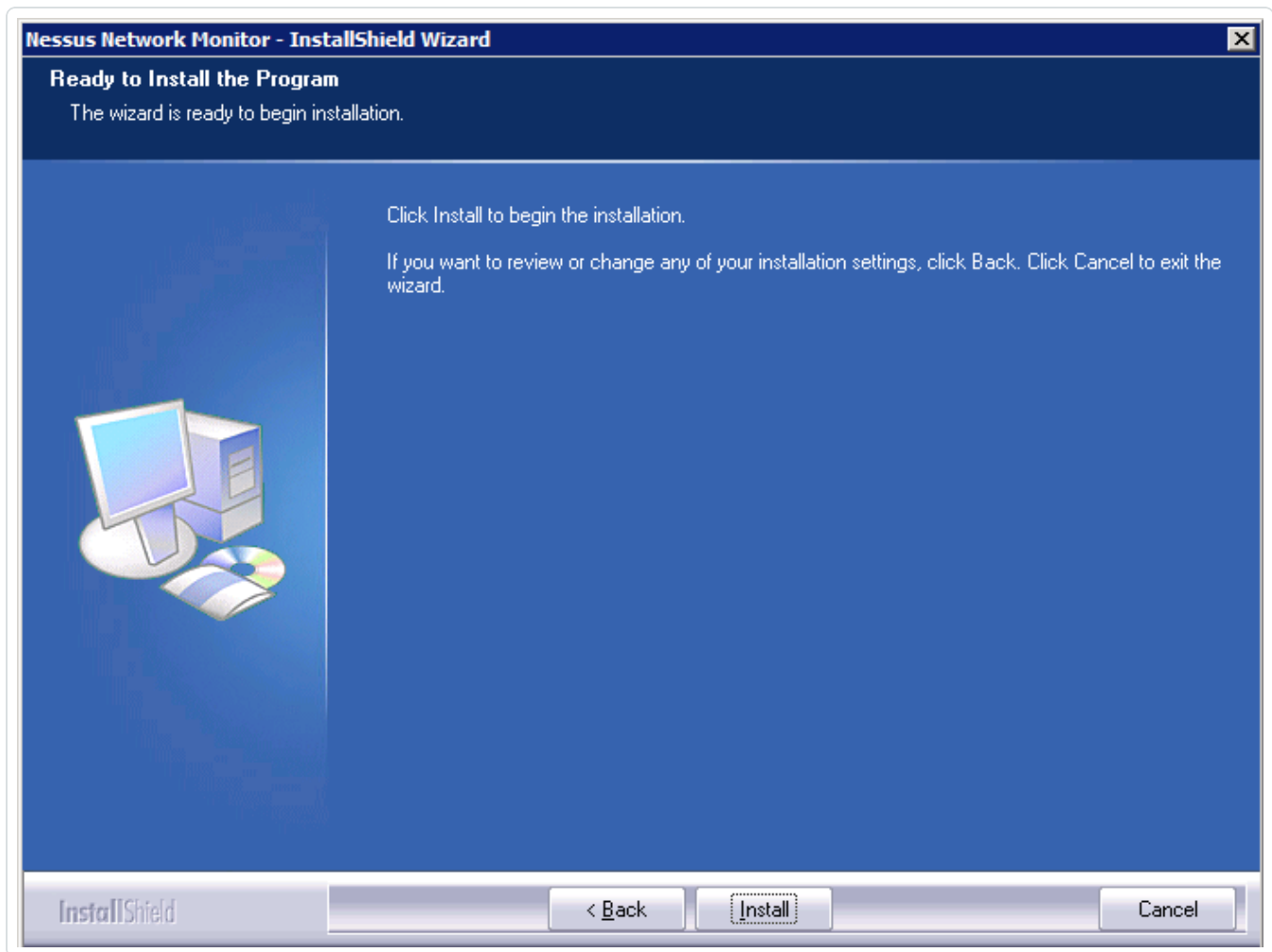


8. Click the **Change** button to specify a custom path.

Tip: If you connect Tenable Nessus Network Monitor to Tenable Security Center, altering the data path disables Tenable Security Center from retrieving reports.

9. Click the **Next** button.

The **Ready to Install the Program** screen appears, where you can review and edit the information supplied on previous screens.



10. Click the **Install** button.

The **Setup Status** screen appears. If the most recent version of WinPcap is already installed on the system, the Tenable Nessus Network Monitor installation process asks if you want to force or cancel installation of WinPcap. If it does not detect WinPcap, or detects an older version, a second installer launches to install or upgrade the software.

Tip: Use the provided version of WinPcap or newer. Tenable Nessus Network Monitor has been designed and tested using the supplied version of WinPcap.

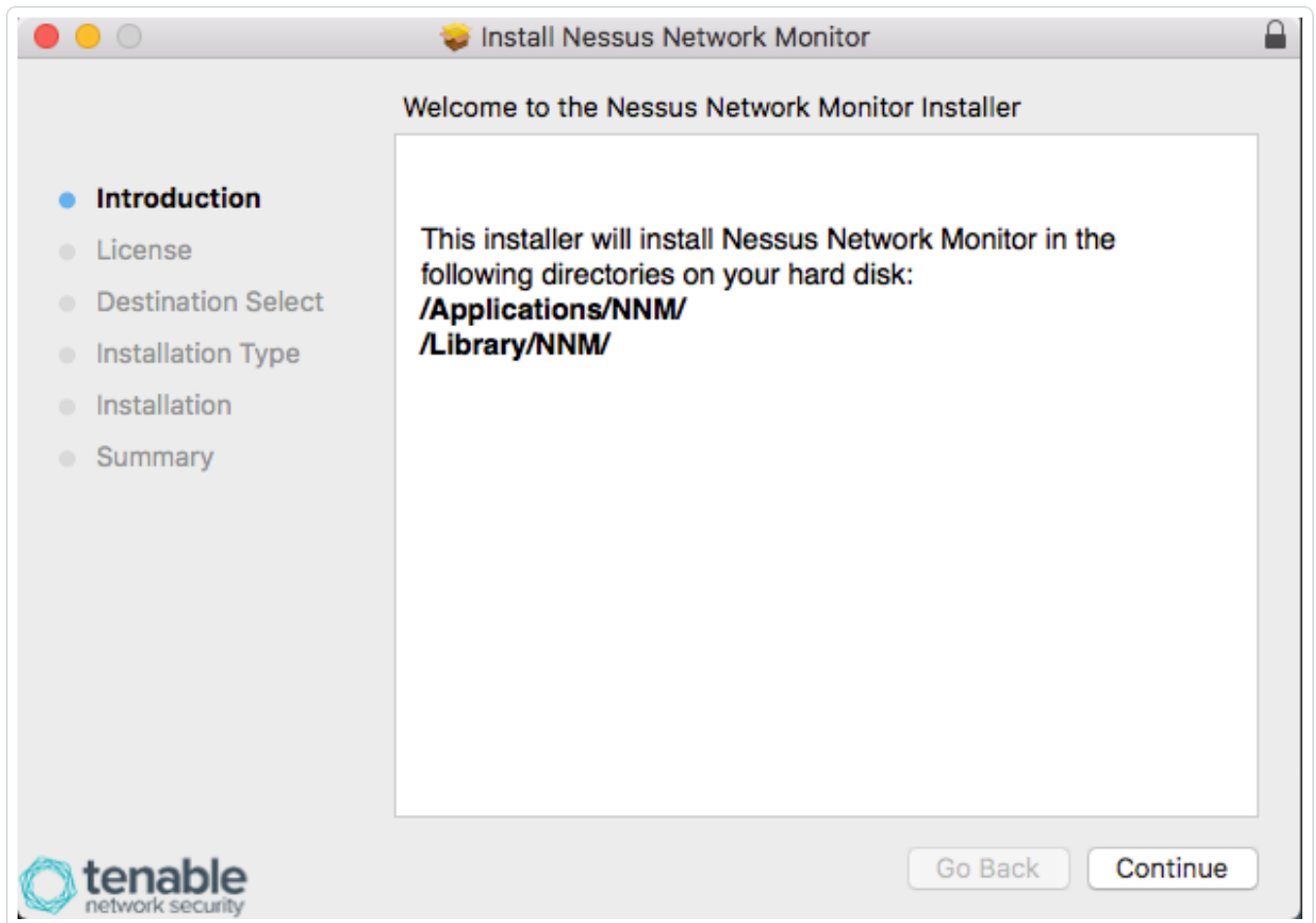
11. [Start Tenable Nessus Network Monitor.](#)

macOS



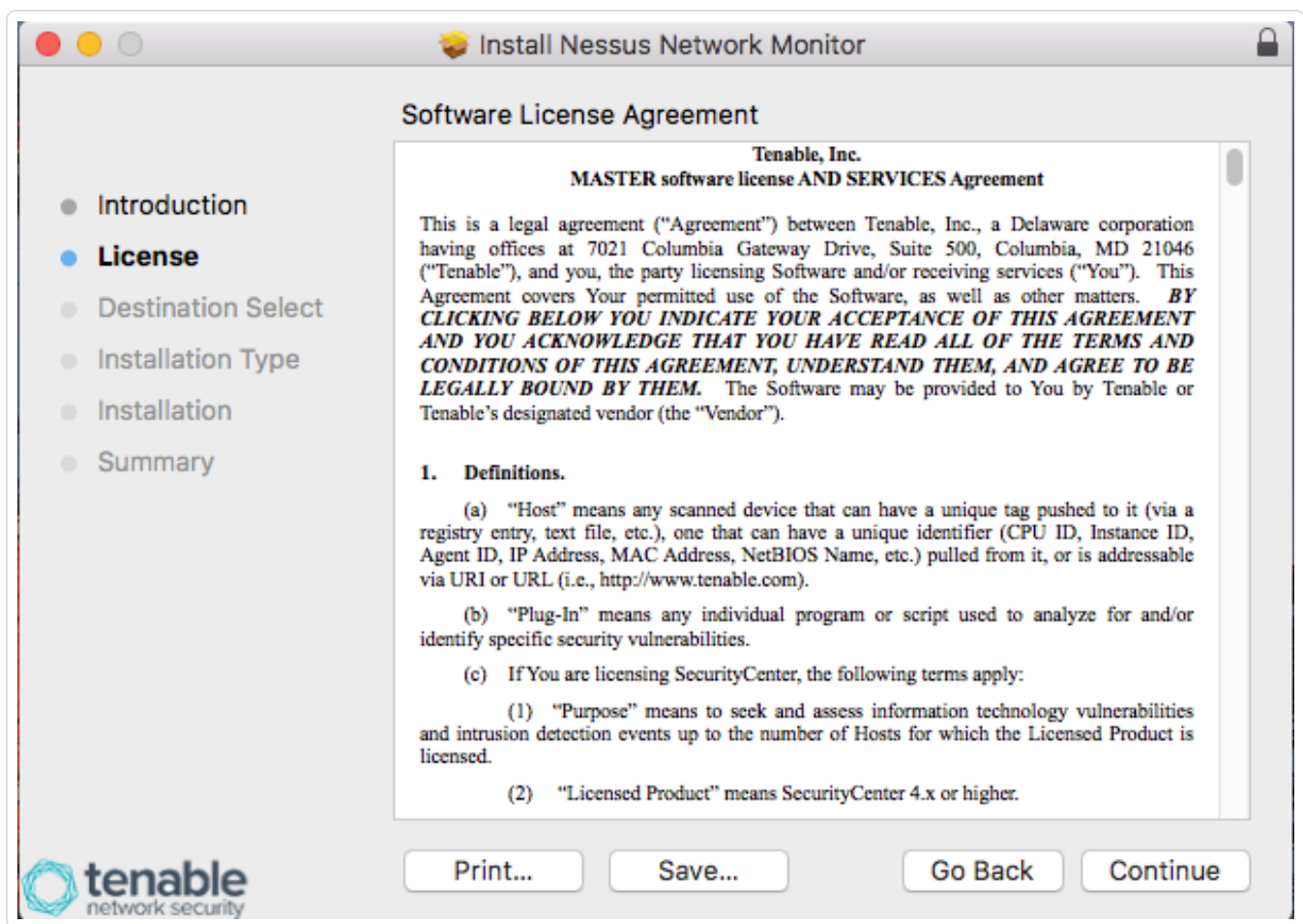
1. Double-click the `.dmg` file downloaded from the [Tenable Downloads](#) page to mount the disk image **Tenable Nessus Network Monitor Install**. The specific filename varies depending on your version.
2. Double-click the **Install Tenable Nessus Network Monitor.pkg** file.

The **Install Tenable Nessus Network Monitor** window appears, which walks you through the installation process and any required configuration steps.



3. Click the **Continue** button.

The **Software License Agreement** screen appears.



4. Agree to the terms to continue the installation process and use Tenable Nessus Network Monitor.

Tip: You can copy the text of the agreement into a separate document for reference, or you can click the **Print** button to print the agreement directly from this screen.

4. Click **Install** to begin the installation.

A window appears asking for authentication permission to install the software.

5. Click the **Install Software** button.

A window appears, requesting permission to allow Tenable Nessus Network Monitor to accept incoming network connections. If this option is denied, Tenable Nessus Network Monitor is installed but functionality is severely reduced.



6. When the identity dialog box appears, click **Continue**.

Tip: Once the installation process is complete, eject the Tenable Nessus Network Monitor install volume.



Upgrade Tenable Nessus Network Monitor

This section describes how to upgrade an existing Tenable Nessus Network Monitor instance on the following platforms:

- [Linux](#)
- [Windows](#)
- [macOS](#)



Upgrade Tenable Nessus Network Monitor on Linux

Before You Begin

These steps assume you have backed up your custom SSL certificates. They also assume that you are running all commands with root privileges.

Additionally, if you have used an Tenable Nessus Network Monitor RPM to install Tenable Nessus Network Monitor previously, an upgrade retains configuration settings. You must transfer the Tenable Nessus Network Monitor RPM package to the system on which it is being installed. Confirm the integrity of the installation package by comparing the download MD5 checksum with the one listed in the product [release notes](#).

To upgrade Tenable Nessus Network Monitor on Linux:

1. Stop Tenable Nessus Network Monitor with the following command:

```
# service nnm stop
```

2. Install the Tenable Nessus Network Monitor `.rpm` file downloaded from the [Tenable Downloads](#) page with the following command. The specific filename varies depending on your version:

```
# rpm -Uvh Tenable Nessus Network Monitor-5.x.x-esx.x86_64.rpm
Preparing...                               ##### [100%]
1:Tenable Nessus Network Monitor #####
[100%]
[*] Tenable Nessus Network Monitor installation completed.
#
```

3. Once the upgrade is complete, start Tenable Nessus Network Monitor with the following command:

```
# service nnm start
```

4. Navigate to `https://<ip address or hostname>:8835`, which displays the Tenable Nessus Network Monitor web front end to log in.

Tip: Ensure that organizational firewall rules permit access to port 8835 on the Tenable Nessus Network Monitor server.



Upgrade Tenable Nessus Network Monitor on Windows

Before You Begin

These steps assume you have backed up your custom SSL certificates. They also assume that you are running all programs as a local user with administrative privileges. To do so, when UAC is enabled, right-click on the installer program and select **Run as Administrator**.

Additionally, you must ensure the latest version of the Microsoft Visual C++ 2010 Redistributable Package is installed for your 64-bit platform and architecture. Be sure to stop any other programs on your system that are utilizing WinPcap.

To upgrade Tenable Nessus Network Monitor on Windows:

1. Stop the Tenable Tenable Nessus Network Monitor Proxy Service from the Windows Services control panel.
2. Double-click the **.exe** file downloaded from the [Tenable Downloads](#) page. The specific file-name varies depending on your platform and/or version.

The InstallShield Wizard launches and begins the upgrade process.

3. Click the **Next** button.

The automated upgrade process begins.

Note: If the version of WinPcap is not at the appropriate level during the upgrade process, an upgrade window appears and begins the process of upgrading WinPcap. Failure to install the recommended version of WinPcap may result in errors with Tenable Nessus Network Monitor monitoring.

4. When the upgrade is complete, [start Tenable Nessus Network Monitor](#).
5. Navigate to **https://<ip address or hostname>:8835** to display the Tenable Nessus Network Monitor web front end to log in.

Tip: Ensure that organizational firewall rules permit access to port 8835 on the Tenable Nessus Network Monitor server.



Upgrade Tenable Nessus Network Monitor on macOS

Before You Begin

These steps assume that you have backed up your custom SSL certificates and are running all programs with root privileges.

To upgrade Tenable Nessus Network Monitor on macOS:

1. [Stop Tenable Nessus Network Monitor](#).
2. Double-click the `.dmg` file downloaded from the [Tenable Downloads](#) page to mount the disk image **NNM Install**. The specific filename varies depending on your version.
3. Double-click the **Install Tenable Nessus Network Monitor.pkg** file.

The Install Tenable Tenable Nessus Network Monitor window appears, which walks you through the upgrade process and any required configuration steps.

4. Click the **Continue** button.

The Software License Agreement screen appears.

5. Agree to the terms to continue the installation process and use Tenable Nessus Network Monitor.

Tip: You can copy the text of the agreement into a separate document for reference, or you can click the Print button to print the agreement directly from this screen.

6. Click the **Install** button.

A window appears asking for authentication permission to install the software.

7. Click the **Install Software** button.

A window appears requesting permission to allow Tenable Nessus Network Monitor to accept incoming network connections. If this option is denied, Tenable Nessus Network Monitor is installed but functionality is severely reduced.

8. Click the **Allow** button.



Set up Tenable Nessus Network Monitor

Tenable Nessus Network Monitor configuration follows the same steps for all operating systems. This section provides instructions for the following:

- [Configure Tenable Nessus Network Monitor](#)
- [Register Tenable Nessus Network Monitor Offline via the Tenable Nessus Network Monitor Interface](#)
- [Register Tenable Nessus Network Monitor Offline via the CLI](#)
- [Configure High Performance Mode](#)



Configure Tenable Nessus Network Monitor

To configure Tenable Nessus Network Monitor:

1. In a web browser, navigate to `https://<ip address or hostname>:8835`.
2. Type the default username and password, which are both **admin**.
3. Click **Sign In To Continue**.
4. The **Change Default Password** screen of the **Quick Setup** window appears, where you can change the default password. The new password must meet the following minimum requirements:
 - Minimum 5 characters long
 - One capital letter
 - One lowercase letter
 - One numeric digit
 - One special character from the following list: `!@#$%^&*()`
5. Click **Next Step**.

The **Set Activation Code** screen appears.

6. To register Tenable Nessus Network Monitor offline, select the **Register Offline** check box and see [Register Tenable Nessus Network Monitor Offline via the CLI](#).
7. In the **Activation Code** box, type the appropriate text based on your setup:
 - If Tenable Nessus Network Monitor is acting as a standalone device, type an Activation Code.
 - If Tenable Nessus Network Monitor is managed by Industrial Security, type **IndustrialSecurity**.

Industrial Security is end-of-life (EOL). For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle [Matrix](#) and [Policy](#).



- a. In the **Industrial Security Host** box, type the IP address of the Industrial Security instance.
 - b. In the **Industrial Security Port** box, type the port of the Industrial Security instance.
 - c. In the **Industrial Security Key** box, type the key copied from the Industrial Security instance. See the [Industrial Security User Guide](#) for more information.
 - d. In the **NNM Name** box, type a name for the Tenable Nessus Network Monitor instance. This name appears in the Industrial Security interface.
- If Tenable Nessus Network Monitor is managed by Tenable Vulnerability Management, type **Cloud**.

Four configuration options appear: **Cloud Host**, **Cloud Port**, **Cloud Key**, and **Tenable Nessus Network Monitor Name**. See the [Cloud Settings section](#) for more information.

- If Tenable Nessus Network Monitor is managed by Tenable Security Center, type **SecurityCenter**. See the [Tenable Security Center User Guide](#) for more information.

In all cases, a valid Activation Code must be typed in the **Activation Code** box.

8. Click **Next Step**.

The **Monitoring Configuration** screen appears.

- The **Monitored Network Interfaces** box displays the monitored interfaces identified by Tenable Nessus Network Monitor. You can select one or more of the defined interfaces. The caret icon displays additional information about each interface.
- The **Monitored Network IP Addresses and Ranges** box displays the IP address ranges Tenable Nessus Network Monitor monitors.
- The **Excluded Network IP Addresses and Ranges** box displays the IP address ranges Tenable Nessus Network Monitor does not monitor.

The **Monitored Network IP Addresses and Ranges** and **Excluded Network IP Addresses and Ranges** boxes accept both IPv4 and IPv6 CIDR address definitions. When using multiple addresses, separate the entries using commas or new lines.



Note: Tenable Network Security does not recommend typing large ranges such as 0.0.0.0/0. Because this indicates to Tenable Nessus Network Monitor that any and all network addresses belong in the network, performance may be severely impacted. Please only include addresses in your network, as each address undergoes in-depth processing.

9. Click **Finish**.

The **Monitoring** page appears. Once Tenable Nessus Network Monitor starts monitoring traffic, the page displays various high-level charts about the vulnerabilities, assets, connections, and bandwidth usage that Tenable Nessus Network Monitor has detected, as well as real-time events that Tenable Nessus Network Monitor has triggered.

Note: By default, Tenable Nessus Network Monitor has discovery mode enabled when installed. You must disable discovery mode for Tenable Nessus Network Monitor to load plugins into memory. For more information on discovery mode, see [Tenable Nessus Network Monitor Settings Section](#).



Verify Your RPM Signature

To verify the rpm's:

1. Download the 4096 signing key at the [Tenable Download Site](#).

You will get a file named **tenable-4096.gpg**.

2. Run the following command to import the file.

```
rpm --import tenable-4096.gpg
```

3. Run the following command to check your downloaded rpm, (for example. nnm-6.1.0-es7.x86_64.rpm).

```
rpm -Kv nnm-6.1.0-es7.x86_64.rpm
```

Tenable Nessus Network Monitor outputs the results of the command. (The 4096 bit key is "V3 RSA/SHA256"):

```
Header V3 RSA/SHA256 Signature, key ID 2f12969d: OK
```

```
Header SHA1 digest: OK (118e3221435977b9ae64b51aab0f2aaef16b0336)
```

```
V3 RSA/SHA256 Signature, key ID 2f12969d: OK
```

```
MD5 digest: OK (491691a5e08510e83757c93eeeb15a1)
```



Register Tenable Nessus Network Monitor Offline via the Tenable Nessus Network Monitor Interface

To register Tenable Nessus Network Monitor offline via the Tenable Nessus Network Monitor interface:

1. During the [Initial Configuration](#), on the **Quick Setup** window, select the **Register Offline** check box.

A challenge code and the **Activation Key** box appear.

The screenshot shows a web interface titled "Quick Setup" with a teal header. Below the header, it says "Step 2 - Set Activation Code". There is a checkbox labeled "Register Offline" which is checked. Below this, there is a line of text: "To create a key, [click here](#) and use the following challenge code:". Underneath this text is a blurred challenge code. Below the challenge code is a text input field labeled "Activation Key". At the bottom of the form, there are two buttons: "Previous Step" on the left and "Next Step" on the right.

2. Copy the challenge code and, in a web browser, navigate to <https://plugins.nessus.org/v2/offline-pvs.php>.
3. In the appropriate boxes, paste your challenge code and type the Activation Code you received from Tenable.
4. Click **Submit**.

The page generates a URL to download the Tenable Nessus Network Monitor plugins tarball. Save this URL, as it is used every time you update your plugins. Additionally, a license key appears.



5. Copy the license key.
6. Navigate to the Tenable Nessus Network Monitor interface.
7. Paste the license key into the **Activation Key** box on the **Quick Setup** window.
8. Click the **Next Step** button.
9. Continue with Step 5 of the [Initial Configuration](#) instructions.

Note: After configuring Tenable Nessus Network Monitor, upload the plugins tarball in the **Offline Update** area of the [Feed Settings](#) section.



Register Tenable Nessus Network Monitor Offline via the CLI

If your Tenable Nessus Network Monitor installation cannot reach the Internet directly, use the following procedure to register and update plugins:

1. On the system running Tenable Nessus Network Monitor, type the following command:

Platform	Command to Run
Red Hat Linux / CentOS	<code># /opt/nnm/bin/nnm --challenge</code>
Windows	<code>C:\Program Files\Tenable\NNM\nnm --challenge</code>
macOS	<code># /Library/NNM/bin/nnm --challenge</code>

This produces a challenge code similar to the following:

```
569ccd9ac72ab3a62a3115a945ef8e710c0d73b8
```

2. Go to <https://plugins.nessus.org/v2/offline-NNM.php>.
3. Paste the challenge code as well as the Activation Code you received previously from Tenable into the appropriate text boxes.

This produces a URL that gives you direct access to the Tenable Nessus Network Monitor plugins.

4. Save the URL as it is used every time you update your plugins.

Additionally, a license key and the associated `NNM.license` file are produced.

5. Copy this file to the host running Tenable Nessus Network Monitor in the appropriate directory.
6. Once the `NNM.license` file is copied, run the `Tenable Nessus Network Monitor --register-offline` command to install the file:

Platform	Directory
Red Hat Linux / CentOS	<code># /opt/nnm/bin/nnm --register-offline /path/to/NNM.license</code>
Windows	<code>C:\Program Files\Tenable\NNM\nnm --register-offline</code>



Platform	Directory
	<code>"C:\path\to\NNM.license"</code>
macOS	<code># /Library/NNM/bin/nmm --register-offline /path/to/NNM.license</code>

7. To obtain the newest plugins, navigate to the URL provided in the previous step.

You receive a TAR file (e.g., `sc-passive.tar.gz`).

8. Copy the file to Tenable Nessus Network Monitor and then type the appropriate command for your platform:

Platform	Command
Red Hat Linux / CentOS	<code># /opt/nmm/bin/nmm --update-plugins /path/to/sc-passive.tar.gz</code>
Windows	<code>C:\Program Files\Tenable\NNM\nmm --update-plugins C:\path\to\sc-passive.tar.gz</code>
macOS	<code># /Library/NNM/bin/nmm --update-plugins /path/to/sc-passive.tar.gz</code>



Register High Performance Mode Tenable Nessus Network Monitor for Tenable Security Center in an Air-gapped Environment

To register Tenable Nessus Network Monitor for Tenable Security Center in an air-gapped environment, you must either update your current install or configure a fresh install of Tenable Nessus Network Monitor

Note: These steps apply to High Performance, 10G mode.

Update the Current Install

From Tenable Nessus Network Monitor:

1. From a CLI on Tenable Nessus Network Monitor, stop the Tenable Nessus Network Monitor service.
2. Run the following command:

```
/opt/nnm/bin/nnm --config "Enable High Performance Mode" "1"
```
3. Start the Tenable Nessus Network Monitor service.
4. In a browser, open Tenable Nessus Network Monitor.
5. Click **Configuration > Feed Settings**.
6. In the **Activation Code** box type 'XXXX'.

Note: This allows the (required) High Performance license to persist and enables the **Fetch Plugins From** drop-down box.

7. From the **Fetch Plugins From** drop-down box, select **SecurityCenter**.
8. Click **Update**.

From Tenable Security Center:

1. Open a browser and [connect to Tenable Security Center](#).
2. Add Tenable Nessus Network Monitor, as described in the [Add a Tenable Nessus Network Monitor](#) in the *Tenable Security Center User Guide*.



3. Click **Submit**.

The system adds Tenable Nessus Network Monitor to Tenable Security Center.

Note: The Tenable Nessus Network Monitor status changes to **Plugins Out of Sync** while the plugins are first downloaded to Tenable Nessus Network Monitor from Tenable Security Center. The next time Tenable Security Center polls Tenable Nessus Network Monitor, the status updates to **Working**.

Configure a Fresh Install

From Tenable Nessus Network Monitor:

1. From a CLI on Tenable Nessus Network Monitor, run the following command:

```
/opt/nnm/bin/nnm --config "Enable High Performance Mode" "1"
```
2. Start the Tenable Nessus Network Monitor service.
3. In a browser, open Tenable Nessus Network Monitor.
4. In Step 2 of the **Quick Setup** steps, check the **Register Offline** check box.
5. In a browser, navigate to <https://plugins.nessus.org/v2/offline.php>.
6. Type the Tenable Nessus Network Monitor challenge code.
7. Type the activation code.
8. In Tenable Nessus Network Monitor complete the **Quick Setup** steps.
9. Click **Configuration > Feed Settings**.
10. In the **Activation Code** box type 'XXXX'.

Note: This allows the (required) High Performance license to persist and enables the **Fetch Plugins From** drop-down box.

11. From the **Fetch Plugins From** drop-down box, select **SecurityCenter**.
12. Click **Update**.

From Tenable Security Center:



1. Open a browser and [connect to Tenable Security Center](#).
2. Add Tenable Nessus Network Monitor, as described in the [Add a Tenable Nessus Network Monitor](#) in the *Tenable Security Center User Guide*.
3. Click **Submit**.

The system adds Tenable Nessus Network Monitor to Tenable Security Center.

Note: The Tenable Nessus Network Monitor status changes to **Plugins Out of Sync** while the plugins are first downloaded to Tenable Nessus Network Monitor from Tenable Security Center. The next time Tenable Security Center polls Tenable Nessus Network Monitor, the status updates to **Working**.



Disable Secure Boot for Tenable Nessus Network Monitor High Performance Mode

On some versions of Linux, the operating system has a Secure Boot option that prevents programs from loading kernel modules. In some versions, such as Red Hat Enterprise Linux 8, Secure Boot is enabled by default. If your Linux operating system has Secure Boot enabled, you must disable Secure Boot mode to run Tenable Nessus Network Monitor in high performance mode.

Note: SELinux is a Linux kernel security module and has rules to prevent programs from loading kernel modules. Tenable Nessus Network Monitor modules comply with these rules, so these security measures are still in place for your system even if you disable Secure Boot.

To disable Secure Boot mode in Red Hat Enterprise Linux:

1. As a root user, access the system's console.
2. To check whether your system has Secure Boot enabled or disabled, type:

```
/usr/bin/mokutil --sb-state
```

If Secure Boot is disabled, you can run Tenable Nessus Network Monitor in High Performance Mode. If Secure Boot is enabled, continue with the rest of the procedure.

2. To disable Secure Boot mode, type:

```
/usr/bin/mokutil --disable-validation
```

The system prompts you for a password.

4. Type a temporary password and confirm the password when prompted.

Tip: Ensure you remember this temporary password because you are required to enter it when you first restart the system after changing the Secure Boot state.

5. To restart the system, type:

```
reboot
```



The system restarts and displays the MOK management screen.

6. On the MOK management screen, press any key to advance.
7. Select **Change Secure Boot state**.
8. Follow the prompts to enter characters from your temporary password.
9. When prompted to disable Secure Boot, select **Yes**.

The system prompts you to restart.

10. Restart your system.

The system restarts with Secure Boot mode disabled. You can now run Tenable Nessus Network Monitor in High Performance mode.

What to do next:

- [Configure High Performance Mode](#)



Configure High Performance Mode

The following steps are required to operate Tenable Nessus Network Monitor in High Performance mode. Alternatively, a user with administrative privileges can enable [High Performance mode via the UI](#).

Tenable Nessus Network Monitor uses multiple cores to process packets received from monitored interfaces. These are known as worker cores. The default number of worker cores is 8. This number can be changed using the configuration parameter **Number Of Worker Cores**.

Note: Tenable Nessus Network Monitor supports a maximum number of 16 cores.

Note: If you set the **Number Of Worker Cores** parameter to 0, Tenable Nessus Network Monitor automatically changes the value to the minimum number of worker cores needed to run Tenable Nessus Network Monitor in High Performance mode.

For example, suppose you have 20 available logical cores. Four of those cores are used by the system for internal processing and the kernel. If you want to use the 16 available cores for Tenable Nessus Network Monitor, then you may change the value for the parameter **Number Of Worker Cores** to 16.

Before you begin:

- Ensure you have a High Performance Activation Code so you can run Tenable Nessus Network Monitor in High Performance mode.
- If you are running Red Hat Enterprise Linux, ensure Secure Boot mode is disabled, as described in [Disable Secure Boot for Tenable Nessus Network Monitor High Performance Mode](#).

To configure High Performance Mode:

1. Stop Tenable Nessus Network Monitor with the following command:

```
# service nnm stop
```

2. Enable High Performance mode with the following command:

```
/opt/nnm/bin/nnm --config "Enable High Performance Mode" "1"
```



3. Confirm that the management network interface is different from the monitoring network interface that you configured initially.

Note: If the configured monitored interface has bound IPv4 addresses, you cannot complete the Quick Setup Wizard to configure Tenable Nessus Network Monitor because no usable NICs appear in the **Monitored Network Interfaces** list.

4. Start Tenable Nessus Network Monitor with the following command:

```
# service nnm start
```

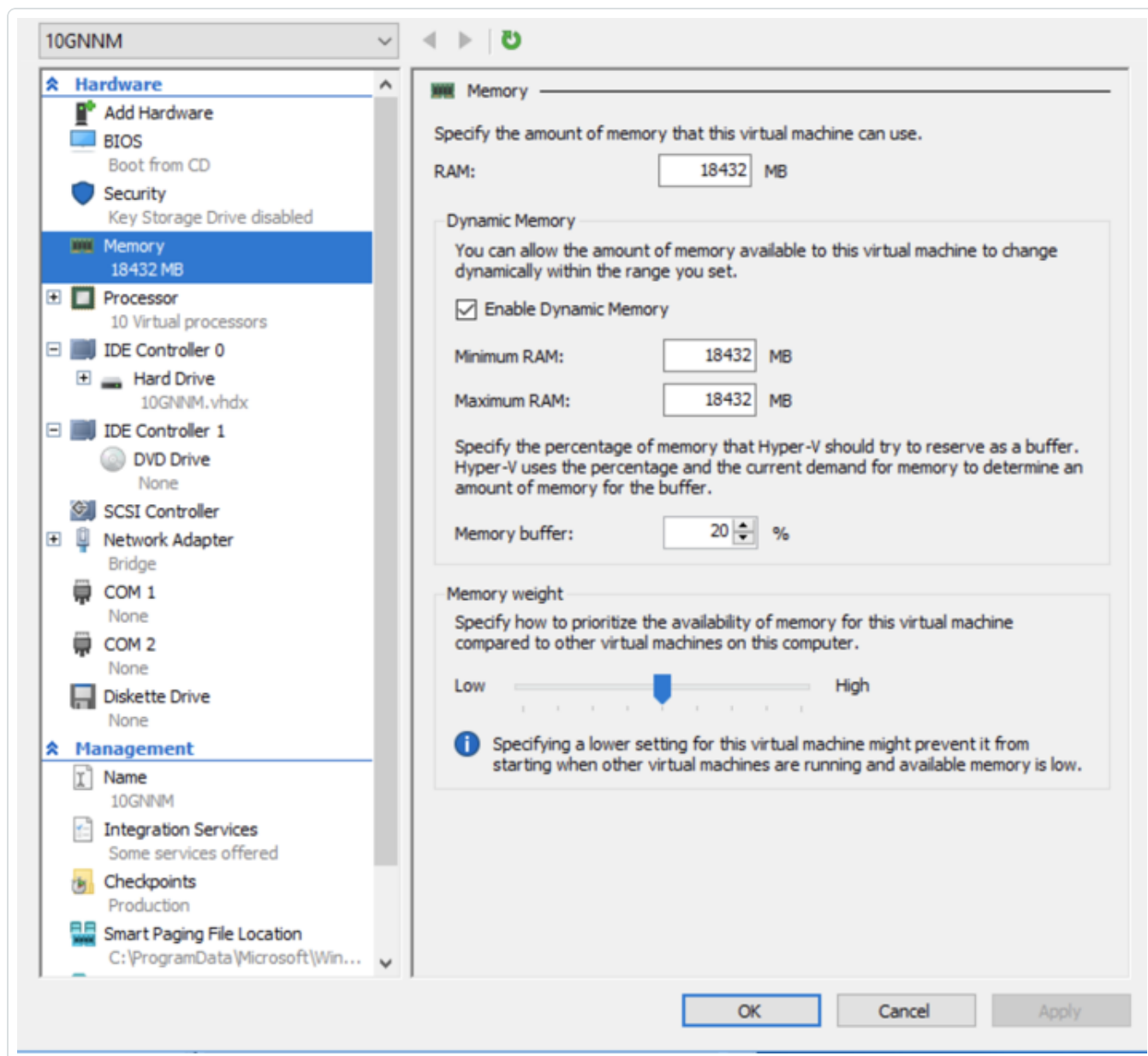


Configure Tenable Nessus Network Monitor in High Performance Mode on Hyper-V

To configure Tenable Nessus Network Monitor in High Performance Mode on Hyper-V:

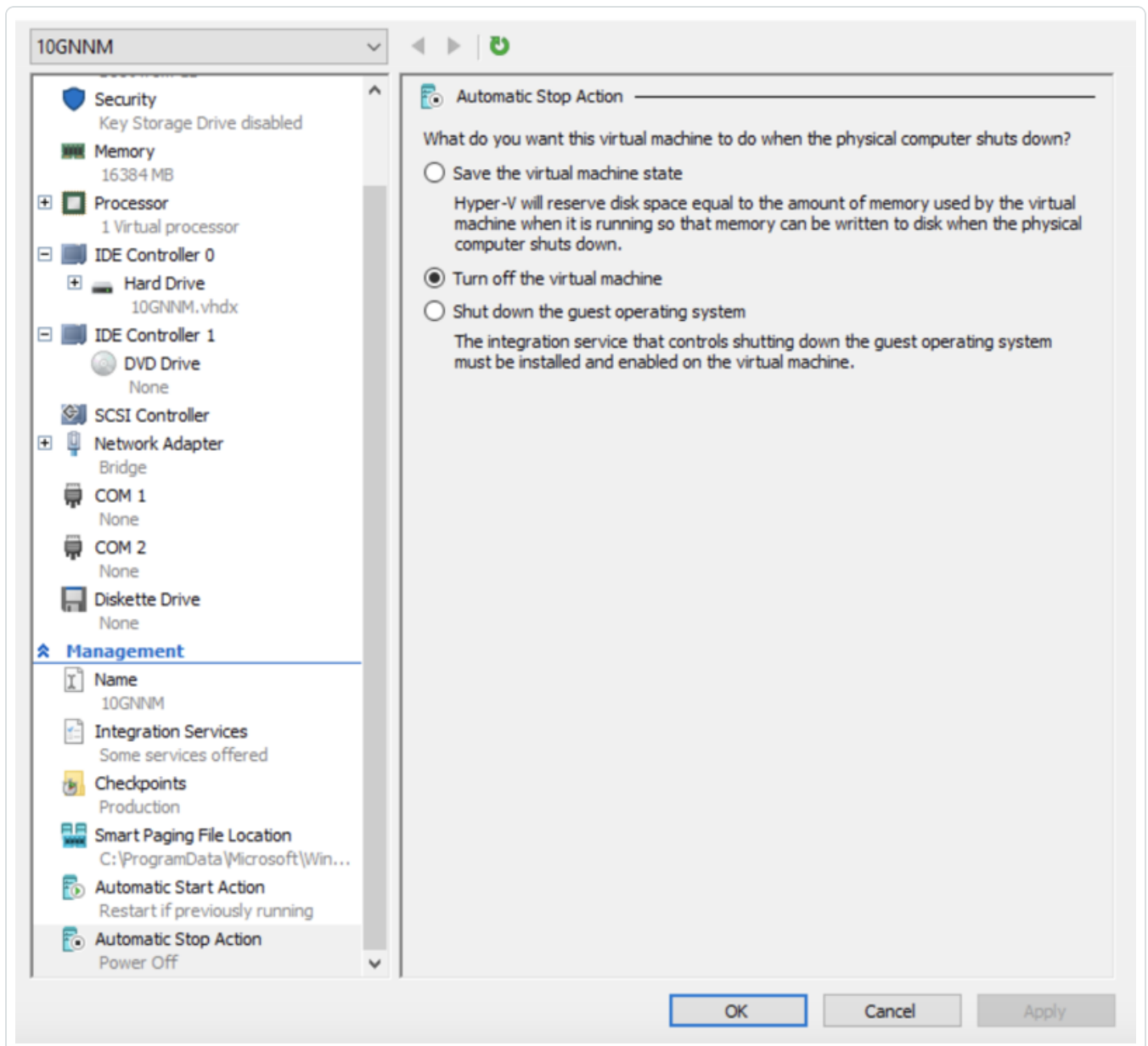
1. Install the CentOS VM.
2. Shut down the VM after install completes.
3. Right click the VM and navigate to **Settings**.

4. In the **Memory** section, check the **Enable Dynamic Memory** check box.



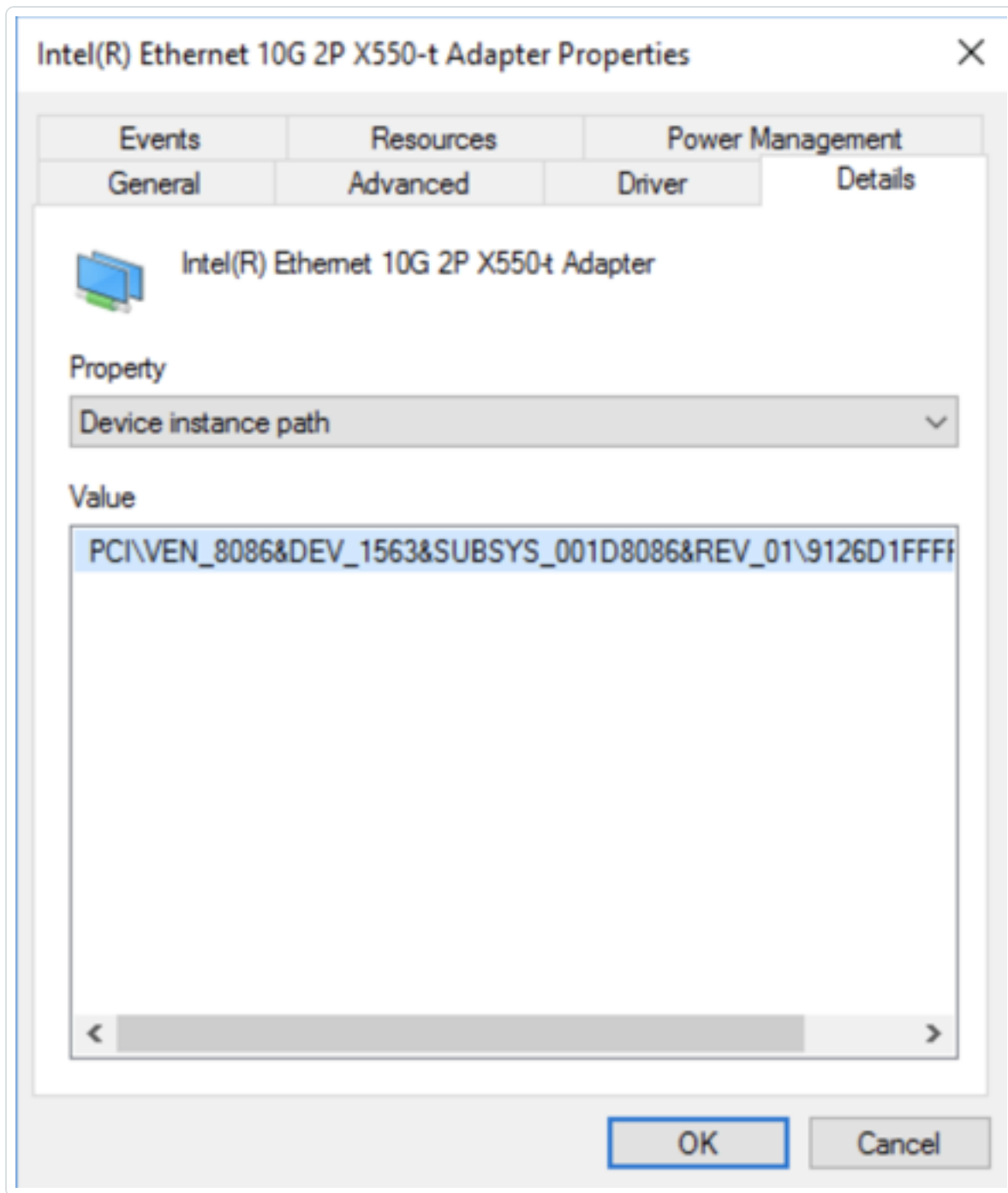
5. Set the **Minimum RAM** to the startup RAM setting.

6. In the **Automatic Stop Action** section, select the **Turn off the virtual machine** radio button.



7. Click **OK**.
8. Open **Device Manager**.
9. Right click on the device you want to configure for passthrough.
10. In the **Properties** dialog, click the **Details** tab.
11. In the **Property** drop-down box, select **Device instance path**.

12. Copy the value from the **Value** box.



13. In Powershell, use the following commands to perform the DDA configuration:

```
# Setting up environment  
# Configure VMName
```




```
$vmName = '10GNNM'

# Configure Instance ID
$instanceId = 'PCI\VEN_8086&DEV_1563&SUBSYS_001D8086&REV_01\9126D1FFFF74000000'

# Configure Extra variable
$vm = Get-VM -Name $vmName
$dev = (Get-PnpDevice -PresentOnly).Where{ $_.InstanceId -like $instanceId }

# Disable device from hosts
Disable-PnpDevice -InstanceId $dev.InstanceId -Confirm:$false

# Setup location path and dismount the device from hosts
$locationPath = (Get-PnpDeviceProperty -KeyName DEVPKEY_Device_LocationPaths -
InstanceId
$dev.InstanceId).Data[0]
echo $locationPath

# Dismount device from the host
Dismount-VmHostAssignableDevice -LocationPath $locationPath -Force -Verbose

# Assign the device to our VM
Add-VMAssignableDevice -VM $vm -LocationPath $locationPath -Verbose
```

Use the following commands if you do not intend to use the device with Tenable Nessus Network Monitor in the VM:

```
# Roll back, shutdown the VM first

# Remove the device from the VM
Remove-VMAssignableDevice -VMName $vmName -Verbose

# Return the device to host
Get-VMHostAssignableDevice | Mount-VmHostAssignableDevice -Verbose

# Enable it in devmgmt.msc
```



```
(Get-PnpDevice -PresentOnly).Where{ $_.InstanceId -like $instanceId }| Enable-  
PnpDevice -Confirm:$false -Verbose
```

14. Turn on the VM.
15. [Install Tenable Nessus Network Monitor](#).
16. Configure huge pages with the commands listed in the [Linux Command Line Operations](#) documentation.
17. [Enable High Performance Mode](#).



Configure Hyper-V NIC in Promiscuous Mode

Hyper-V NIC configured in promiscuous mode allows you to monitor external traffic.

1. Open Powershell.
2. Run the following command to add a VMSwitch Port Feature, where "LAN2" is your virtual switch name.

```
SettingData.MonitorMode = 2)
$A=Get-VMSwitchExtensionPortFeature -FeatureName "Ethernet Switch Port
Security Settings"
(OR $A = Get-VMSwitchExtensionPortFeature -FeatureId 776e0ba7-94a1-41c8-
8f28-951f524251b5)
$A.SettingData.MonitorMode = 2
Add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName LAN2 -
VMSwitchExtensionFeature $A
```

3. Run the following command to change the PortMirroring Attribute of the VM Networkdevice, where "VMName 06_WinXPMonitor" is your VM name and "00155D016612" is the MAC address of your adapter.

```
Get-VMNetworkAdapter -VMName 06_WinXPMonitor | ? MacAddress -eq '00155D016612' |
Set-VMNetworkAdapter -PortMirroring Destination
```

See [How to Expand the Size of Disk Volume](#) for more information.



Configure Tenable Nessus Network Monitor on Machines Hosting Napatech Acceleration Cards

If you use the Napatech Link™ Capture Software v11.30 package, you can configure your machine to use Tenable Nessus Network Monitor in High Performance Mode to acquire network traffic from your hardware acceleration devices. For more information, see [Configure High Performance Mode](#).

Note: Tenable Nessus Network Monitor only supports this feature on Red Hat 7 or CentOS 7 platforms because they use the latest performance improvements of the Linux Kernel.

Requirements

Product	Manufacturer	Operating System	Comments
Tenable Nessus Network Monitor 5.10+	Tenable, Inc.®	RH7 or CentOS7	Requires High Performance Mode licensing
Napatech Link™ Capture Software v11.3.0	Napatech Inc.	RH7 or CentOS7	Napatech product number: 810-0048-09-10

To configure the Napatech deployment:

1. [Download Napatech Link](#).
2. In a text editor, append the following line to the `/etc/bashrc` file:

```
export NAPATECH3_PATH=/opt/napatech3
```

3. Deploy `ntanl_package_3gd-11.3.0-linux.tar.gz` as follows in `/tmp` or any temporary directory by running the following command:

```
tar xfz ntanl_package_3gd-11.3.0-linux.tar.gz
cd ntanl_package_3gd-11.3.0-linux
package_install_3gd-11.3.0.sh --noprompt
/opt/napatech3/bin/ntstart.sh
```



4. Do one of the following:

- If the Napatech software reports any issues, contact Napatech Support.
- If the Napatech software does not report any issues, run the following command:

```
/opt/napatech3/bin/ntstop.sh
```

To configure the Tenable Nessus Network Monitor deployment:

1. Do one of the following:

- For a new deployment, run the following command:

```
rpm -i nnm-5.10.0-es7.x86_64.rpm
```

Note: In this example, the Tenable Nessus Network Monitor version is 5.10.0. Please ensure this version number matches the version you want to install.

- For an existing deployment, run the following command:

```
rpm -U nnm-5.10.0-es7.x86_64.rpm
```

Note: In this example, the Tenable Nessus Network Monitor version is 5.10.0. Please ensure this version number matches the version you have installed.

HugePages Configuration

During installation, the file `/opt/napatech3/config/ntservice.ini` is automatically updated to include the following line:

```
# [How many, page_size, NUMA_ID]  
HostBuffersRx = [16,16,-1]
```

Verify that the `/opt/napatech3/config/ntservice.ini` file contains the line; otherwise, edit the file manually to include the line.



Troubleshoot Issues with Napatech in Tenable Nessus Network Monitor

Cannot engage Tenable Nessus Network Monitor in High Performance Mode from the UI

If you are unable to engage Tenable Nessus Network Monitor in High Performance Mode from the UI or command line:

1. Check the Tenable Nessus Network Monitor log file at `/opt/nnm/var/nnm/logs/yyyymm.log` where `yyyymm` is the year and month (for example, `/opt/nnm/var/nnm/logs/201909.log`)
2. If you see a **Cannot Create Ring for Worker Core X** message, edit the `/opt/napatech3/config/ntservice.ini` file to match the **Number of Worker Cores** configured in the [Tenable Nessus Network Monitor Settings Section](#).
3. Restart the `ntservice` and `nnm` services.

No Traffic seen in Tenable Nessus Network Monitor UI

1. Run the following command to display the traffic going through the Napatech card:

```
/opt/napatech3/bin/monitoring
```

2. If you see traffic in the Napatech card but not in the Tenable Nessus Network Monitor user interface, perform the following steps:

- a. Run the following command:

```
kill -10 `cat /var/run/nnm.pid`
```

- b. Run the following command, where `yyyymm` is the year and month (for example, `/opt/nnm/var/nnm/logs/201909.log`):

```
less /opt/nnm/var/nnm/logs/yyyymm.log
```



- c. Go to the bottom of the file. If you see messages like the following, then you must restart the the ntsservice and nsm services:

```
Sep 11, 2019 10:38:32 (NNM Core) [INFO] NIC port 0: received: 2098625  
Sep 11, 2019 10:38:32 (NNM Core) [INFO] Worker core 1 (Rx core 0, NIC port 0): processed: 0  
Sep 11, 2019 10:38:32 (NNM Core) [INFO] Worker core 2 (Rx core 0, NIC port 0): processed: 0  
...
```



Remove Tenable Nessus Network Monitor

The following instructions describe how to remove Tenable Nessus Network Monitor from the following platforms:

- [Linux](#)
- [Windows](#)
- [macOS](#)



Remove Tenable Nessus Network Monitor from Linux

To remove Tenable Nessus Network Monitor from Linux:

1. Stop Tenable Nessus Network Monitor with the following command:

```
# service nnm stop
```

3. Remove the Tenable Nessus Network Monitor RPM with the following command:

```
# rpm -e NNM
```

4. Some user-created and user-modified files are not removed with the `-e` command. Remove any remaining files with the following command:

```
# rm -rf /opt/nnm
```

Tenable Nessus Network Monitor is removed.



Remove Tenable Nessus Network Monitor from Windows

To remove Tenable Nessus Network Monitor from Windows:

1. Depending on your version of Windows, in the **Control Panel**, under **Programs**, click one of the following:

- **Programs and Features**
- **Add or Remove Programs**

2. Select **Tenable Tenable Nessus Network Monitor**.

3. Click **Change/Remove**.

The InstallShield Wizard appears.

4. Follow the directions in this wizard to completely remove Tenable Nessus Network Monitor.

5. Select **Yes** to remove the Tenable Nessus Network Monitor program and all its files, folders, and features from the system.

-or-

Select **No** to remove only the Tenable Nessus Network Monitor program. All user-created files and relevant file folders remain on the system.

6. Restart your machine to complete the removal.

7. Follow the same instructions to remove WinPcap.



Remove Tenable Nessus Network Monitor from macOS

To remove Tenable Nessus Network Monitor from macOS:

1. [Stop Tenable Nessus Network Monitor](#).
2. Delete the following directories (including subdirectories) and files with either sudo root or root privileges using the command line:

```
# rm /Library/LaunchDaemons/com.tenablesecurity.nnm*
# rm -r /Library/NNM
# rm -r /Library/PreferencePanes/NNM*
# rm -r /Applications/NNM
```

Tenable Nessus Network Monitor is removed from your macOS system.



Monitoring Page

The **Monitoring** page provides a centralized view of vulnerabilities discovered by Tenable Nessus Network Monitor. On this page, vulnerabilities may be viewed in several categories, including **Dashboards**, **Hosts**, **Vulnerabilities**, **Applications**, **Operating Systems**, **Connections**, and **Mobile Devices**. The results may also be exported in different formats for use in other programs.

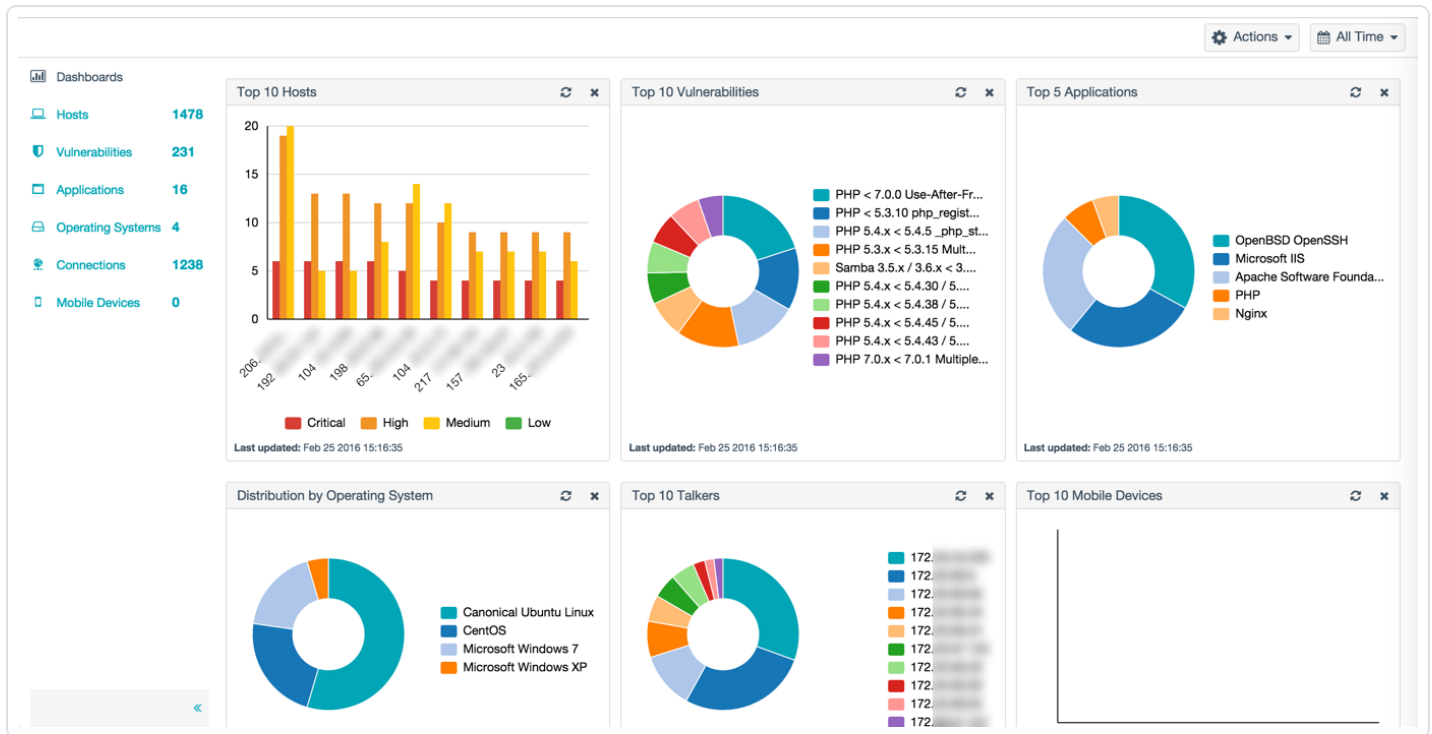
Across all of the viewable methods available on the **Monitoring** page, filter options are available to increase granularity when viewing results. Click the heading of a column to sort items within that section of the **Monitoring** page in ascending or descending order.

The **Actions** drop-down box allows you to export results, delete results, or launch a Tenable Nessus scan.

Note: After deleting results, you must restart Tenable Nessus Network Monitor to see the most up-to-date information.

The **Filter <section name>** box allows for quick filtering of the **Monitoring** page. To view a list of filterable plugin attributes, click the down arrow for any quick filter box. Results appear based on a match of **Any** or **All** filters. The search box contains example hints when empty, but if an incorrect filter value is introduced, the box displays a red border.

Note: The **Filter <section name>** box is not available in the **Dashboards** section.



Filter Text

Name	Description
Bugtraq ID	Filter the results of discovered vulnerabilities based on their Bugtraq identifications.
CPE	Filter the results of discovered vulnerabilities based on their CPE identifiers.
CVE	Filter the results of discovered vulnerabilities based on their CVE identifiers.
CVSS Base Score	Filter the results of discovered vulnerabilities based on the base CVSS score as reported by vulnerability plugins.
CVSS Temporal Score	Filter the results of discovered vulnerabilities based on the temporal CVSS score as reported by vulnerability plugins.
CVSS Temporal Vector	Filter the results of discovered vulnerabilities based on the CVSS temporal vector as reported by vulnerability plugins.



Name	Description
CVSS Vector	Filter the results of discovered vulnerabilities based on the CVSS vector as reported by vulnerability plugins.
CVSS v3.0 Base Score	Filter the results of discovered vulnerabilities based on the CVSS v3.0 base score as reported by vulnerability plugins.
CVSS v3.0 Temporal Score	Filter the results of discovered vulnerabilities based on the temporal CVSS v3.0 score as reported by vulnerability plugins.
CVSS v3.0 Temporal Vector	Filter the results of discovered vulnerabilities based on the temporal CVSS v3.0 vector as reported by vulnerability plugins.
CVSS v3.0 Vector	Filter the results of discovered vulnerabilities based on the CVSS v3.0 vector as reported by vulnerability plugins.
Host	Filter the results of discovered vulnerabilities based on the discovered IP address of the device.
IAVA ID	Filter the results of discovered vulnerabilities based on the IAVA IDs of the vulnerabilities.
IAVB ID	Filter the results of discovered vulnerabilities based on the IAVB IDs of the vulnerabilities.
IAVT ID	Filter the results of discovered vulnerabilities based on the IAVT IDs of the vulnerabilities.
OSVDB ID	Filter the results of discovered vulnerabilities based on the discovered OSVDB identifiers.
Plugin Description	Filter the results of discovered vulnerabilities based on text available in the descriptions of the vulnerabilities.
Plugin Family	Filter the results of discovered vulnerabilities based on a family of discovered vulnerabilities.
Plugin ID	Filter the results of discovered vulnerabilities based on the IDs of the plugins that identified the vulnerabilities.



Name	Description
Plugin Name	Filter the results of discovered vulnerabilities based on text available in the names of the plugins that identified the vulnerabilities.
Plugin Output	Filter the results of discovered vulnerabilities based on text contained in the output of the plugin that discovered the vulnerability.
Port	Filter the results of discovered vulnerabilities based on the port on which the vulnerability was discovered.
Protocol	Filter the results of discovered vulnerabilities based on the detected protocol: tcp, udp, or icmp.
STIG Severity	Filter the results of discovered vulnerabilities based on STIG severity level of the plugin.
See Also	Filter the results of discovered vulnerabilities based on the text available in the See Also box of the plugin.
Severity	Filter the results of discovered vulnerabilities based on the identified severity.
Solution	Filter the results of discovered vulnerabilities based on text available in the solution section of the plugin.
Synopsis	Filter the results of discovered vulnerabilities based on text available in the synopsis section of the plugin.
System Type	Filter the results of discovered vulnerabilities based on the system type of the device.
VLAN ID	Filter the results of discovered vulnerabilities based on the VLAN ID of the device.



Dashboards Section

The **Dashboards** section displays the contents of the vulnerability tab in a graphical layout. The default dashboard layout displays the following charts:

- Top 10 Hosts
- Top 10 Vulnerabilities
- Top 5 Applications
- Distribution by Operating System
- Top 10 Talkers

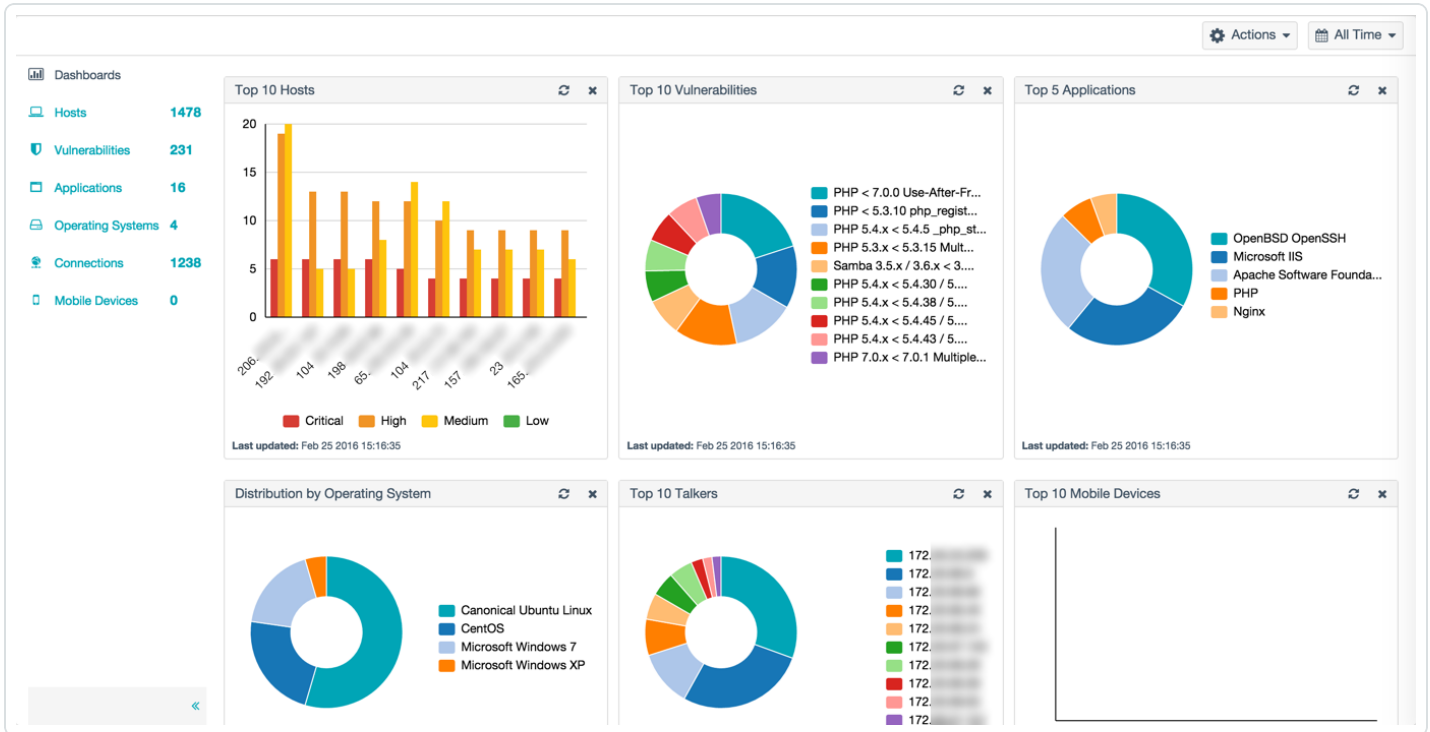
Note: The 10 Top Talkers chart only lists client machines that call or talk to the servers. If you are interested in viewing both servers and clients, enable the **Enable Connection Analysis Module** setting in the [Tenable Nessus Network Monitor Settings Section](#).

- Top 10 Mobile Devices
- Distribution of Mobile Devices by Operating System
- Top 10 Mobile Devices by Hardware
- Distribution of Mobile Applications by Application
- SCADA Vulnerability Distribution by Severity
- Top 10 SCADA Hosts
- SCADA Host Distribution by Protocol
- SCADA Host Distribution by System Type
- Client Connections
- Network Bandwidth by Byte Count
- Event Trending

Note: Your Tenable Nessus Network Monitor configuration determines which charts appear in the **Dashboards** section.



Click on the data within a chart to see more information about the data. Additionally, you can drag-and-drop charts to rearrange them on the dashboard for the duration of your session. The **Client Connections**, **Network Bandwidth by Byte Count**, and **Event Trending** charts cannot be moved. For more information, see [Rearrange Charts](#).



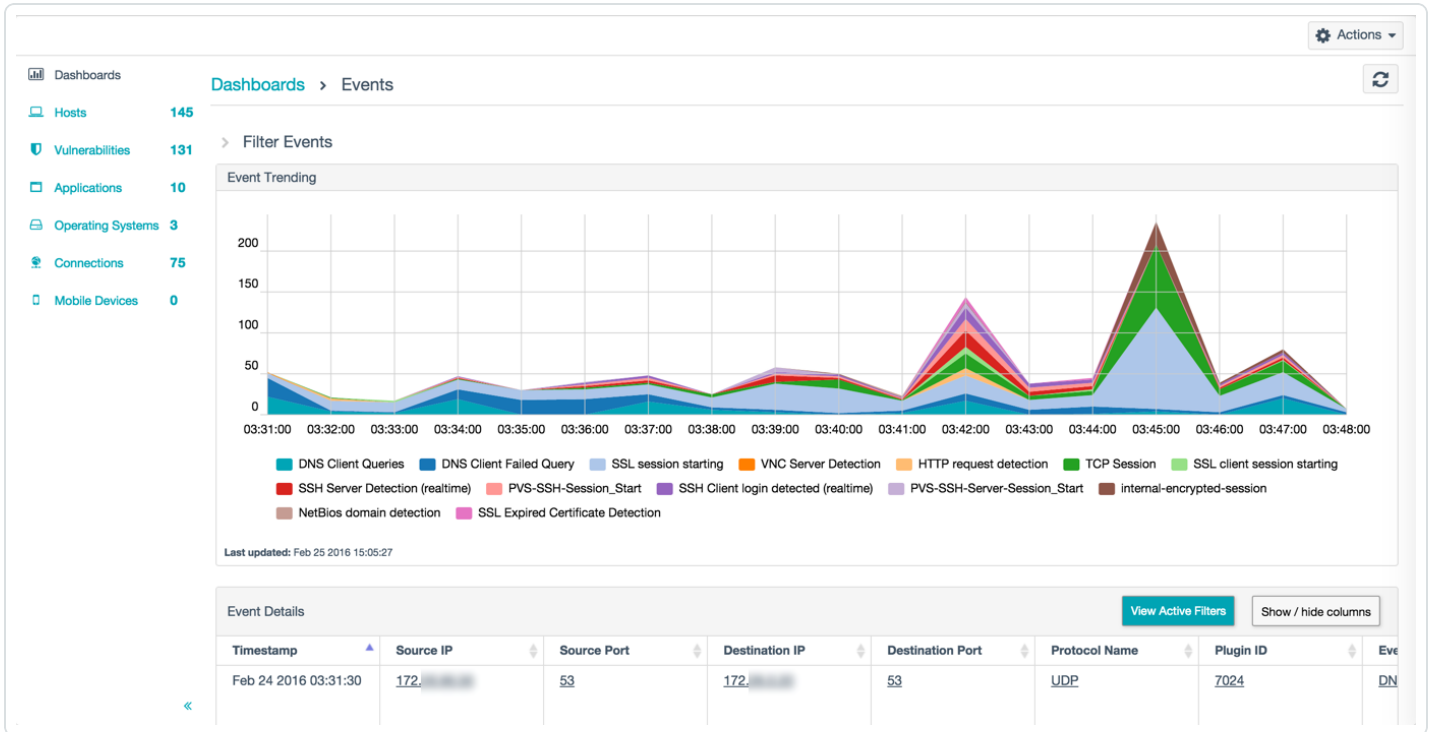
The following table describes the options available in the **Dashboards** section:

Option	Description
<click on the chart>	Opens a Details section with more information about the data displayed in a chart. Note: You cannot click on the Top 10 Mobile Devices by Hardware chart.
✕ button	Removes the chart from the Dashboards section for the duration of your session.
↻ button	Refreshes the chart.
⚙ button	Provides options to Export Results , Delete Results , or Launch Scan .
📅 button	Provides options to filter chart data based on a specified date range.



Events Dashboard

Click on the **Event Trending** chart to Access the **Events** dashboard. The **Events** dashboard displays a graphical representation of the number of maximum viewable real-time events as defined in the **Realtime Events** setting type in the **Tenable Nessus Network Monitor Settings** section.



The **Event Details** table can be customized by sorting columns, showing or hiding columns, filtering content by clicking **View Active Filters**, or by clicking underlined columns in the table.



Rearrange Charts

To rearrange charts on the Dashboard:

1. In the **Dashboards** section, select the heading of the chart you want to reposition.
2. Drag the chart to a different location on the dashboard.
3. Release the pointer.


The chart moves and the dashboard configuration saves for the duration of your session.

Note: You cannot move the **Client Connections**, **Network Bandwidth by Byte Count**, or **Event Trending** charts.



Refresh a Chart

To refresh a chart on the Dashboard:


1. In the **Dashboards** section, in the upper right corner of the chart you want to refresh, click the  button.

The selected chart refreshes.



Set a Date Range for the Dashboards Section

To set a date range for the charts on the Dashboard:

1. In the **Dashboards** section, in the upper right corner, click the  drop-down box.
2. Do one of the following:
 - Select one of the preset time intervals.
 - Select a start and end date from the available calendars and specify a time associated with each date.
 - Manually type dates in the two text boxes in YYYY/MM/DD format and specify a time associated with each date.

All the charts on the page refresh to reflect the selected time interval.



Remove a Chart from a Dashboard

To remove a chart from a dashboard:

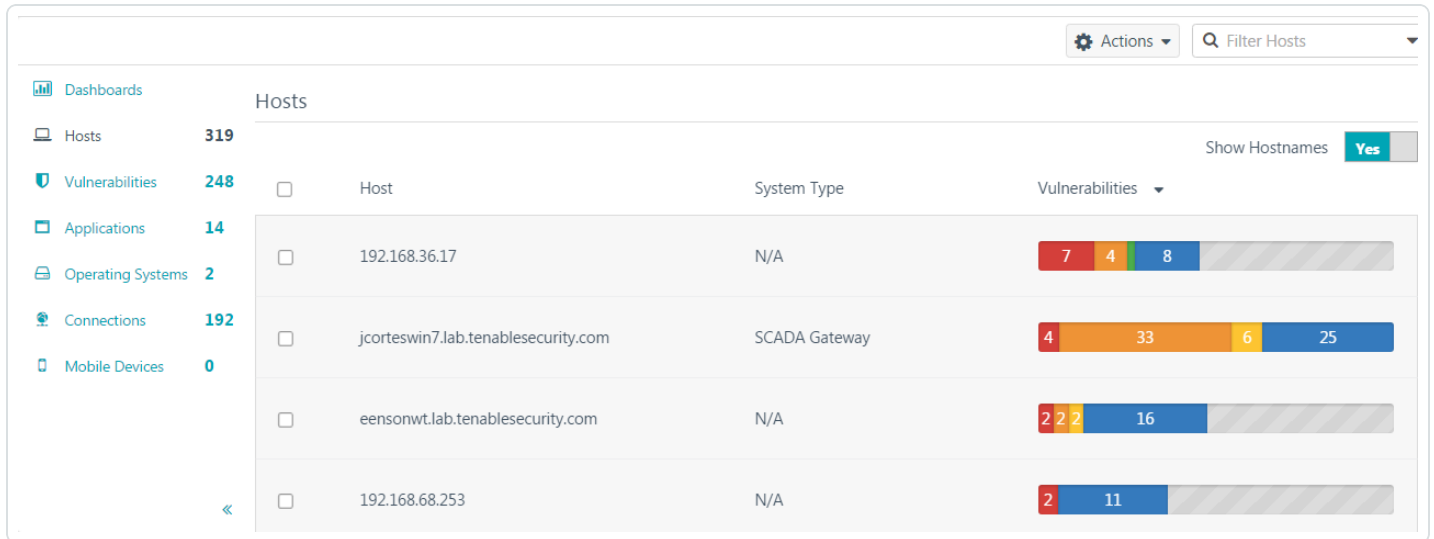
In the **Dashboards** section, in the upper right corner of the chart you want to remove, click the ✖ button.

The selected chart is removed from the dashboard for the duration of your session.



Hosts Section

The **Hosts** section of the **Monitoring** page displays a list of the discovered hosts, the system type of the hosts, and a stacked bar chart. The chart is labeled and color-coded to indicate both the number and severity level of vulnerabilities detected on the host.



Select a host from the list to display the host's attributes and discovered vulnerabilities. In the drop-down box at the top of the section, select one of the following options to view relevant information.

Vulnerabilities

Vulnerabilities detected on this host appear in descending order of severity. The **Vulnerabilities** list displays the name of each vulnerability, the vulnerability family, and the number of vulnerabilities discovered. Select a vulnerability from the list to display vulnerability details including a synopsis, a description, a solution, plugin details, risk information, reference information, and affected hosts and services for the host.



Actions Filter Vulnerabilities

Dashboards Hosts > 206. Vulnerabilities

Hosts 1518 Vulnerabilities 259 Applications 16 Operating Systems 4 Connections 1291 Mobile Devices 0

Severity	Plugin Name	Plugin Family	Count
CRITICAL	PHP < 7.0.0 Use-After-Free Vuln...	Web Servers	1
CRITICAL	PHP 5.4.x < 5.4.30 / 5.5.x < 5.5.1...	Web Servers	1
CRITICAL	PHP 5.4.x < 5.4.38 / 5.5.x < 5.5.2...	Web Servers	1
CRITICAL	PHP 5.4.x < 5.4.43 / 5.5.x < 5.5.2...	Web Servers	1
CRITICAL	PHP 5.4.x < 5.4.45 / 5.5.x < 5.5.2...	Web Servers	1
CRITICAL	PHP 7.0.x < 7.0.1 Multiple Vulner...	Web Servers	1
HIGH	OpenSSL < 0.9.8o / 1.0.0a Multi...	Web Servers	1
HIGH	OpenSSL < 0.9.8za / < 1.0.0m / ...	Web Servers	1
HIGH	OpenSSL < 0.9.8zb / < 1.0.0n / <...	Web Servers	1
HIGH	OpenSSL < 0.9.8zc / < 1.0.0o / <...	Web Servers	1
HIGH	OpenSSL 0.9.8 < 0.9.8s / 1.x < 1...	Web Servers	1
HIGH	PHP 5.4.x < 5.4.32 / 5.5.x < 5.5.1...	Web Servers	1

Host Details

IP: 206. ...
Hostname: 206-...
MAC: c4-...
Last Seen: Feb 19 2016 16:08:31

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Applications

Applications appear in descending order of severity. The **Applications** list displays the name and number of each application. Select an application from the list to display information about the application observed on this host. The list includes the name and number of discoveries, the affected port and protocol, the software and version, and the services available.



Actions Filter Applications

Dashboards Hosts > 206 Applications

Hosts 1518 Vulnerabilities 259 Applications 16 Operating Systems 4 Connections 1291 Mobile Devices 0

Severity	Application Name	Count
CRITICAL	PHP	1
HIGH	OpenSSL Project OpenSSL	1
MEDIUM	Apache Software Foundation Apache HTTP Server	1

Host Details

IP: 206
Hostname: 206
MAC: c4
Last Seen: Feb 19 2016 16:08:31

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Client Connections

Hosts to which the selected host has connected are grouped by port. The **Client Connections** list displays information about connections from the selected host to other hosts, which port(s) were used, and, if known, the services. Click on a client connection to display a **Connections** sidebar that displays **Host Details**, a **Client Connections** diagram, and, where applicable, a **Recent Sessions** table.



Sort Affected Ports Actions Filter Affected Ports

Hosts > 172 > Client Connections

Internal Client Trusted Connection

Description

The following internal TCP connections were discovered from 172

Affected Ports (39)

Port	Output	Count
Port 47779		1
47779 / tcp / unkno...	TCP connection(s) detected from 172 to the following 1 server(s): 172	
Port 47894		1
47894 / tcp / unkno...	TCP connection(s) detected from 172 to the following 1 server(s): 172	
Port 47908		1
47908 / tcp / unkno...	TCP connection(s) detected from 172 to the following 1 server(s): 172	

Host Details

IP: 172
Hostname: stash
MAC: c4
Last Seen: Feb 25 2016 12:25:09

Client Connections Diagram

View Connections By: Server Hosts

Client: 172 39

Server Host	Count
172	19
172	7
172	6
172	3
172	2
172	2

Server Connections

Hosts that have connected to the selected host are grouped by port. The **Server Connections** list displays information about connections to the selected host from other hosts, which port(s) were used, and, if known, the services. Click on a server connection to display a **Connections** sidebar that displays **Host Details**, a **Server Connections** diagram, and, where applicable, a **Recent Sessions** table.



Sort Affected Ports Actions Filter Affected Ports

Dashboards Hosts 1518 Vulnerabilities 259 Applications 16 Operating Systems 4 Connections 1291 Mobile Devices 0

Hosts > 206 > Server Connecio...

Internal Server Trusted Connection

Description

The following internal TCP connections were discovered to 206

Affected Ports (1)

Port	Output
80 / tcp / http	TCP connection(s) detected from the following 1 client(s) to 206 : 172

Host Details

IP: 206
Hostname: 206
MAC: c4:
Last Seen: Feb 19 2016 16:08:31

Server Connections Diagram

View Connections By: Client Hosts

Server: 206

172



Vulnerabilities Section

The **Vulnerabilities** section of the **Monitoring** page provides a list of the vulnerabilities detected by Tenable Nessus Network Monitor. Additionally, you can view a vulnerability's plugin family and the number of detected vulnerabilities.

Severity	Plugin Name	Plugin Family	Count
CRITICAL	Samba 3.5.x / 3.6.x < 3.6.25 / 4.0.x < 4.0.25 / 4.1.x < 4.1.17 / 4.2.x < 4.2rc5 TALLOC_FREE() RCE	Samba	6
CRITICAL	Samba 3.x < 3.6.4 / 3.5.14 / 3.4.16 RPC Multiple Buffer Overflows	Samba	1
HIGH	Apache 2.2 < 2.2.17 Multiple Vulnerabilities	Web Servers	1
HIGH	Apache 2.2 < 2.2.20 Multiple Vulnerabilities	Web Servers	1
HIGH	Apache 2.2 < 2.2.21 mod_proxy_ajp DoS	Web Servers	1
HIGH	OpenSSH < 4.4 Multiple GSSAPI Vulnerabilities	SSH	1
HIGH	OpenSSH < 4.7 Trusted X11 Cookie Connection Policy Bypass	SSH	1
HIGH	Samba < 3.6.22 / 4.0.13 / 4.1.3 Multiple Vulnerabilities	Samba	1
HIGH	Samba < 3.6.23 / 4.0.16 / 4.1.6 Multiple Vulnerabilities	Samba	1
MEDIUM	OpenSSH < 5.7 Multiple Vulnerabilities	SSH	9
MEDIUM	Samba 3.6.x < 3.6.24 / 4.0.x < 4.0.19 / 4.1.x < 4.1.9 Multiple Vulnerabilities	Samba	6
MEDIUM	TLS Export-Grade Key Exchange Detection	Generic	4
MEDIUM	Recursive DNS Server Detection	DNS Servers	2

Select a vulnerability from the list to view the following vulnerability details:

- A **Synopsis** of the vulnerability.
- A **Description** of the vulnerability.
- A **Solution** for the vulnerability.
- A **See Also** section that features additional reference material about the vulnerability.
- A list of **Affected Hosts**.
- The vulnerability's **Plugin Details**.
- **Risk Information** about the vulnerability.
- **Reference Information** about the vulnerability.



Delete a Vulnerability

To delete a vulnerability:

To delete one vulnerability:

1. In the **Vulnerabilities** section, hover over the vulnerability you want to delete.
2. On the right side of the row, click the **✕** button.

The vulnerability is deleted.

To delete multiple vulnerabilities:

1. On the **Vulnerabilities** page, on the left side of the row for the vulnerability you want to delete, select the check box. Repeat this step for each vulnerability you want to delete.
2. Click **Actions > Delete Vulnerabilities**.

The vulnerabilities are deleted.



SIEM Analysis Section

Security Information and Event Management (SIEM) analysis allows you to import data from SIEM providers (for example, Splunk) to evaluate events that may warrant re-scanning the affected hosts.

Note: SIEM analysis features are only available for RH/CentOS 7 and RH/CentOS 8. Additionally, discovery mode must be turned off to view SIEM analysis features (see [Tenable Nessus Network Monitor Settings Section](#) for more information).

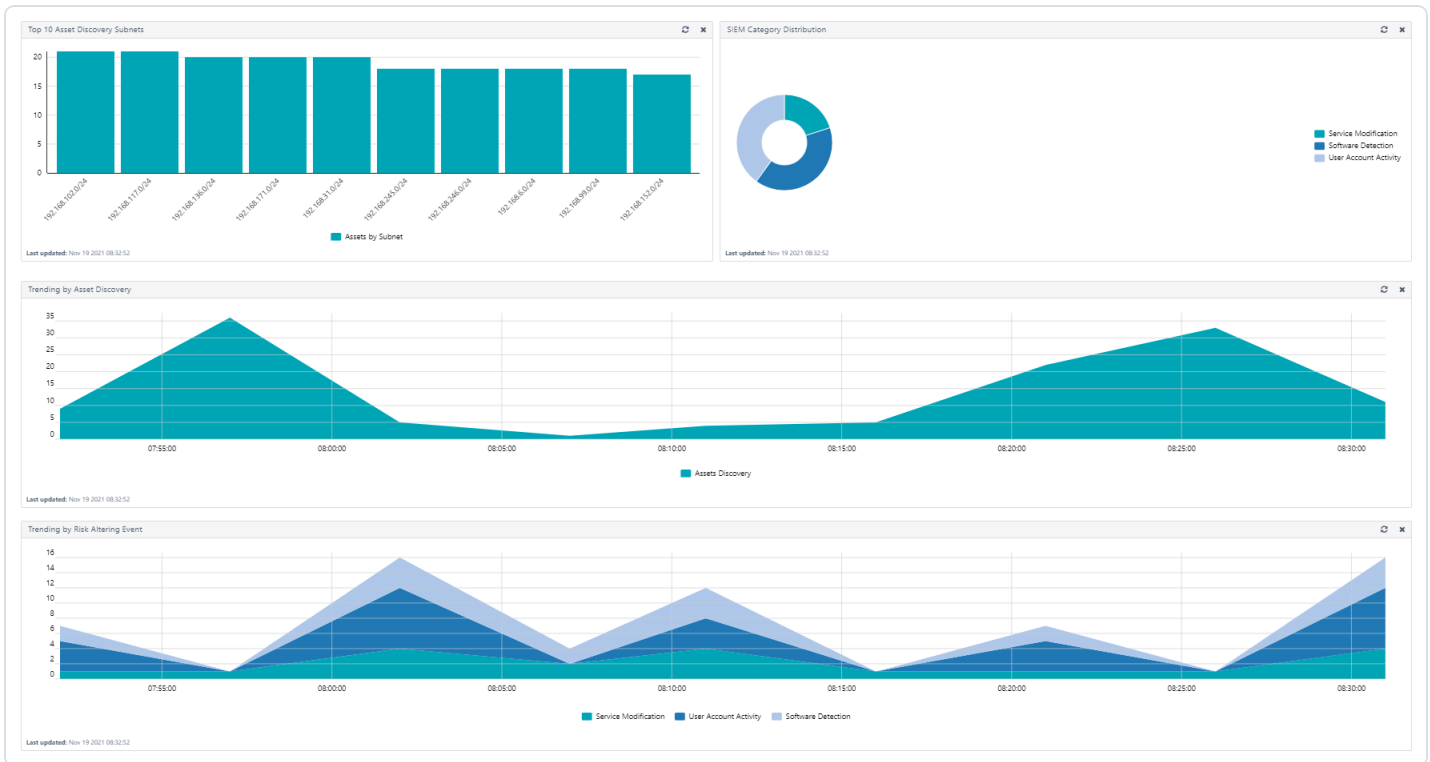
Note: You must deploy Tenable Nessus Network Monitor using the RPM appropriate to your site to activate the SIEM analysis feature.

Note: Tenable recommends that you only use trusted self signed certs for Splunk instances that are used with Tenable Nessus Network Monitor.

The **SIEM Analysis** section of the **Monitoring** page shows four charts that help you track and understand SIEM-related events occurring in your system:

- **Top 10 Asset Discovery Subnets**
- **SIEM Category Distribution**
- **Trending by Asset Discovery**
- **Trending by Risk Altering Event**

Note: The data collection that creates these charts can be configured in the **SIEM Processing Options** and **SIEM Servers** settings. See [Tenable Nessus Network Monitor Settings Section](#) for more information.



The **SIEM Category Distribution** and **Trending by Risk Altering Events** show data based on the risk-altering events discovered in your system. There are **four risk-altering event types**:

Event Type	Description
Assets Discovery	Instances where assets are discovered using DHCP events.
User Account Activity	Instances where a user account on an asset is modified in one of the following ways: <ul style="list-style-type: none">• Account is created or deleted• Account is added or removed to/from a group• Account password modified• Policy that affects user accounts is modified (i.e. password policy, lockout policy)
Software Detection	Instances where software is added or removed by a user or the software management system. For example:



	<ul style="list-style-type: none">• RPM installations• Software added via YUM• Installations on Windows using standard install tools <p>Note: This type does not include instances where binaries are copied on the system and run without execution.</p>
Service Modification	Instances where the software service is modified in one of the following ways: <ul style="list-style-type: none">• Service starts or stops• Service fails to start• Service reboots• Service is installed or uninstalled



Applications Section

The **Applications** section displays a list of discovered applications. Click an application to display a list of affected hosts. The list includes the name and number of discoveries, the affected port and protocol, the software and version, and the services available.

⚙️ Actions ▾ 🔍 Filter Applications ▾

- 📄 Dashboards
- 🖨️ Hosts 152
- 🛡️ Vulnerabilities 79
- 📁 Applications 8
- 📦 Operating Systems 1
- 🌐 Connections 74
- 📱 Mobile Devices 1

Applications

Severity ▾	Application Name	Count
CRITICAL	Samba Samba	5
HIGH	OpenBSD OpenSSH	12
HIGH	Apache Software Foundation Apache HTTP Server	1
MEDIUM	Haxx Curl	1
INFO	baseurl yum	5
INFO	Apple Safari	1
INFO	Google Chrome	1
INFO	Mozilla Firefox	1

«



Operating Systems Section

The **Operating Systems** section displays a list of discovered operating systems. This section lists the severity, operating system name as detected, and the number of discoveries.

Click an operating system to display a list of affected hosts. The list includes the severity, the version of the operating system, and the services available.

Operating Systems

Severity	Operating System Name	Count
INFO	CentOS	3



Connections Section

The **Connections** section displays information in two tabs:

- The **Client Connections** tab displays a list of hosts. Click on a host to display connections from the selected host to other hosts, the port(s) used, and, if known, the services. Additionally, the **Connections** sidebar displays **Host Details**, a **Client Connections** diagram, and, where applicable, a **Recent Sessions** table.
- The **Server Connections** tab displays a list of hosts. Click on a host to display connections to the selected host from other hosts, the port(s) used, and, if known, the services. Additionally, the **Connections** sidebar displays **Host Details**, a **Server Connections** diagram, and, where applicable, a **Recent Sessions** table.

Severity	IP Address	Hostname	Count
INFO	172.20.98.53	N/A	1
INFO	172.20.128.100	stash corp.tenablesecurity.com	5
INFO	172.20.128.87	lap-1114.corp.tenablesecurity.com	2
INFO	172.20.128.130	tns-1040.corp.tenablesecurity.com	1
INFO	172.20.128.134	tns-1194.corp.tenablesecurity.com	1
INFO	172.20.133.86	tns-1070.corp.tenablesecurity.com	1
INFO	172.20.133.86	tns-1070.corp.tenablesecurity.com	2
INFO	172.20.20.120	N/A	1
INFO	172.20.98.8	N/A	2
INFO	172.20.98.13	N/A	2
INFO	172.20.98.14	N/A	1
INFO	172.20.98.15	N/A	1
INFO	172.20.98.14	N/A	1



Mobile Devices Section

The **Mobile Devices** section displays a list of discovered mobile devices. The summary page displays the IP address, model, operating system, and last seen timestamp for each mobile device within the monitored network range. Select a device name from the list to display the device's list of vulnerabilities and a list of applications for the mobile device.

⚙️ Actions ▾ 🔍 Filter Mobile Devices ▾

Dashboards

Hosts **152**

Vulnerabilities **79**

Applications **8**

Operating Systems **1**

Connections **74**

Mobile Devices **1**

Mobile Devices

Show Hostnames **Yes**

<input type="checkbox"/>	Host	Model	Operating System	Last Seen ▾
<input type="checkbox"/>	tns[REDACTED]	N/A	Apple iPhone OS	Jan 19 2016 16:16:10

[⏪](#)



Filter Monitoring Results

To filter monitoring results:

1. In the **Hosts**, **Vulnerabilities**, **Applications**, **Operating Systems**, **Connections**, or **Mobile Devices** section, in the upper right corner, click the **Filter <section name>** drop-down box.
2. Type the criteria by which you want to filter results directly into the box.

-or-

Click the ▼ button in the box.

The **Filter Results** window appears.

Match **All** of the following filters. Display **3** filters per page.

Bugtraq ID	is equal to	NUMBER	×
Host	is not equal to	IP Address	×
STIG Severity	contains	STIG Severity (ie: IV)	×

Page **1** / 1

Apply Filters **Close** **Add Filter** **Clear Filters**

3. Configure the filter options as necessary.
4. Click the **Apply Filters** button.

Note: On-the-fly filter results cannot be exported. If you want to export filter results, you must configure the filter(s) in the **Filter Results** window. Additionally, on-the-fly filter results are not stored when a user navigates to another page in Tenable Nessus Network Monitor.



Export Monitoring Results

To export monitoring results:

1. Click **Monitoring > Actions > Export Results**.

The **Export Results** screen appears.

Export Results

Export Format

Chapters

2. Select the export format and chapter layout.
3. Click the **Export** button.

An automatic download begins. You can save the report from the web browser.

Note: On-the-fly filter results cannot be exported. If you want to export filter results, you must configure the filter(s) in the **Filter Results** window.



Launch a Tenable Nessus Scan

To launch a Tenable Nessus scan:

1. Do one of the following:
 - Click **Monitoring > Actions > Launch Scan**.
 - Click **Assets** or **Vulnerabilities** > select the check boxes for the assets you want to scan > **Actions > Launch Scan**.

The **Launch Basic Nessus Scan** window appears.

2. Configure the scan options as necessary.
3. Click the **Launch** button.

The scan opens in the Tenable Nessus interface. Refer to the [Tenable Nessus user guide](#) for further instructions.

Note: To launch scans on Tenable Nessus 6.8.x or higher, Tenable Nessus Network Monitor must be configured to restrict access to TLS 1.2 or higher. See the [Tenable Nessus Network Monitor Settings Section](#) for more information.



Results Page

The **Results** page contains snapshots of monitored data, results from Pcap files entered manually via the command line or the client UI, and uploaded Tenable Nessus Network Monitor reports. The **Monitoring Snapshots** generate regularly based on the **Report Frequency** setting. They are stored until deleted or the **Report Lifetime** setting removes them. Select a result grouping to view it using the same analysis tools described in the **Monitoring** section of this user guide:

- Hosts
- Vulnerabilities
- Applications
- Operating Systems
- Connections
- Mobile Devices

Additionally, to compare two snapshots, check the desired snapshot results and select the **Diff Snapshots** option from the **Actions** drop-down box.

<input type="checkbox"/>	Result Title	Upload Time	Last Updated	Result Type
<input type="checkbox"/>	Monitoring Snapshot - Jan 20 2016 10:47:41	January 20, 2016 10:47:41	January 20, 2016 10:47:41	Snapshot
<input type="checkbox"/>	Monitoring Snapshot - Jan 20 2016 10:32:41	January 20, 2016 10:32:41	January 20, 2016 10:32:41	Snapshot
<input type="checkbox"/>	Monitoring Snapshot - Jan 20 2016 10:17:41	January 20, 2016 10:17:41	January 20, 2016 10:17:41	Snapshot
<input type="checkbox"/>	Monitoring Snapshot - Jan 20 2016 10:02:41	January 20, 2016 10:02:41	January 20, 2016 10:02:41	Snapshot
<input type="checkbox"/>	Monitoring Snapshot - Jan 20 2016 09:47:41	January 20, 2016 09:47:41	January 20, 2016 09:47:41	Snapshot
<input type="checkbox"/>	Monitoring Snapshot - Jan 20 2016 09:32:41	January 20, 2016 09:32:41	January 20, 2016 09:32:41	Snapshot
<input type="checkbox"/>	Monitoring Snapshot - Jan 20 2016 09:17:41	January 20, 2016 09:17:41	January 20, 2016 09:17:41	Snapshot
<input type="checkbox"/>	Monitoring Snapshot - Jan 20 2016 09:02:41	January 20, 2016 09:02:41	January 20, 2016 09:02:41	Snapshot
<input type="checkbox"/>	Monitoring Snapshot - Jan 20 2016 08:47:41	January 20, 2016 08:47:41	January 20, 2016 08:47:41	Snapshot
<input type="checkbox"/>	Monitoring Snapshot - Jan 20 2016 08:32:41	January 20, 2016 08:32:41	January 20, 2016 08:32:41	Snapshot
<input type="checkbox"/>	Monitoring Snapshot - Jan 20 2016 08:17:41	January 20, 2016 08:17:41	January 20, 2016 08:17:41	Snapshot
<input type="checkbox"/>	Monitoring Snapshot - Jan 20 2016 08:02:41	January 20, 2016 08:02:41	January 20, 2016 08:02:41	Snapshot
<input type="checkbox"/>	Monitoring Snapshot - Jan 20 2016 07:47:41	January 20, 2016 07:47:41	January 20, 2016 07:47:41	Snapshot



Upload a Report

To upload a report:

1. Click **Results > Upload > Report**.

The **Upload Results** window appears.

2. Select a file to upload.

3. Click the **Upload Results** button.

The report appears in a new row at the top of the **Listing Results** list on the **Results** page.



Upload a Pcap

Before You Begin

The maximum total file size for uploaded Pcaps is 100 MB. Running a Pcap pauses live monitoring.

To upload a Pcap:

1. Click **Results > Upload > Pcaps**.

The **Upload Pcaps** window appears.

2. Select one or more files to upload.
3. Click the **Upload Pcap(s)** button.

A new row for the Pcap(s) appears at the top of the **Listing Results** list on the **Results** page.



Filter Results

To filter results:

1. On the **Results** page, in the upper right corner, click the **Filter Results** drop-down box.
2. Select **Snapshot**, **Manual**, or **Pcap**.

The **Listing Results** list filters by the selected report type. Click **Clear Filter** to remove the filter from the list.



Delete Results

To delete one result:

1. On the **Results** page, hover over the result you wish to delete.
2. Click the **x** button.

A dialog box appears confirming your selection to delete the result.

3. Click the **Delete** button.

The result is deleted.

To delete multiple results:

1. On the left side of the row for the result you want to delete, select the check box. Repeat this step for each result you want to delete.
2. Click **Actions > Delete Result**.

A dialog box appears confirming your selection to delete the results.

3. Click the **Delete** button.


The resultss are deleted.



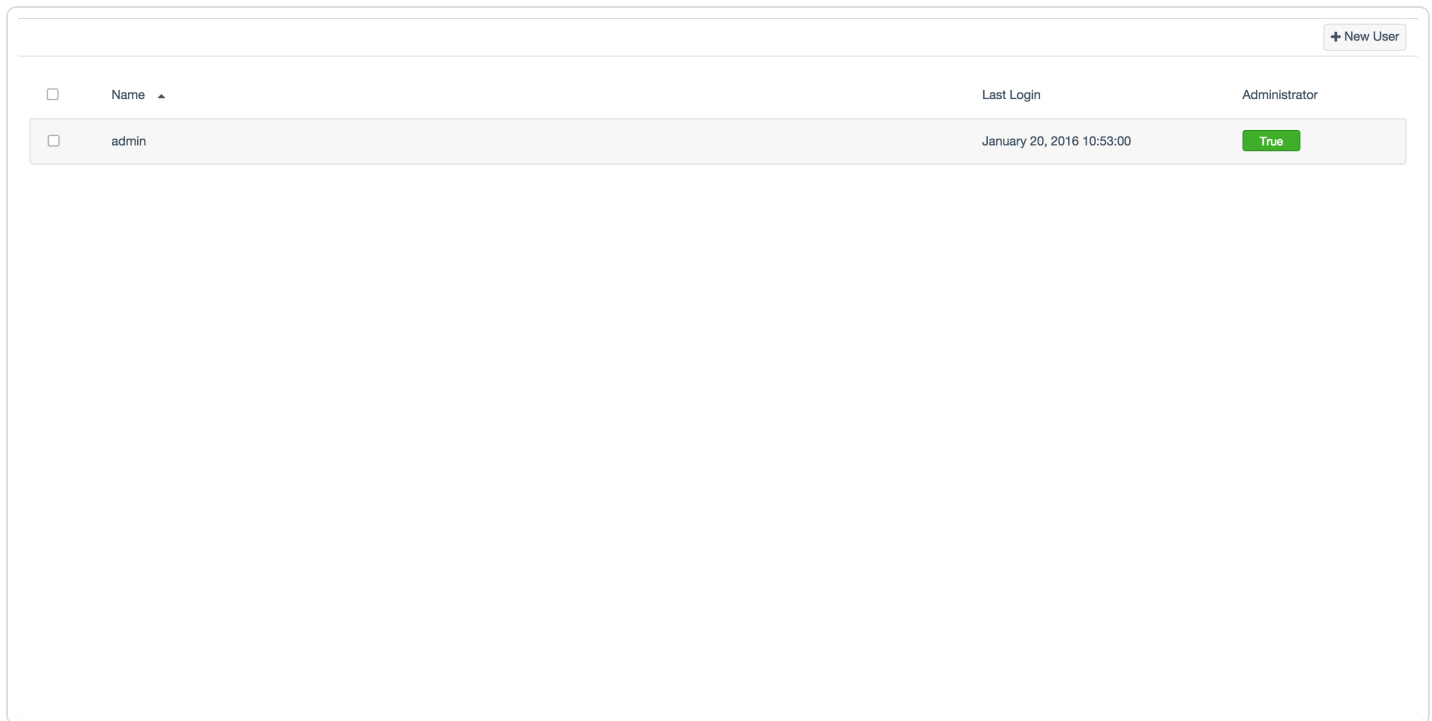
Users Page

The **Users** page lists the available users on the Tenable Nessus Network Monitor server. Also, you can view account configuration options for each user. This page is visible only to users with administrative privileges.

To access the Users page:

1. In the top navigation bar, click the  icon.
2. In the drop-down box, click **Users**.

The **Users** page appears.



<input type="checkbox"/>	Name ▲	Last Login	Administrator
<input type="checkbox"/>	admin	January 20, 2016 10:53:00	True

Click on a user modify the user's account. For more information, see [Modify a User Account](#).

Note: Tenable Nessus Network Monitor complies with STIG APSC-DV-001740. Tenable Nessus Network Monitor stores a cryptographic representation of user passwords (rather than storing the cleartext passwords themselves) in its encrypted database. These passwords are encrypted with salted cryptographic hashes which have no useful value to an attacker.



Create a New User

To create a new user:

1. On the **Users** page, in the upper right corner, click the **New User** button.

The **New User** window appears.

The screenshot shows a 'New User' dialog box with the following fields and controls:

- Username**: Text input field with placeholder text 'Username'.
- Password**: Text input field with placeholder text 'Password'.
- Confirm Password**: Text input field with placeholder text 'Confirm Password'.
- Administrator**: Check box, currently unchecked.
- Create User**: Teal button.
- Cancel**: Grey button.

2. In the **Username** box, type a username for the user.
3. In the **Password** box, type a password for the user.

Note: The username is case sensitive and the password must conform to the Tenable Nessus Network Monitor password policy:

- Minimum length of five characters
- At least one uppercase character
- At least one lowercase character
- At least one number
- At least one of the following special characters: ! @ # \$ % ^ & * ()

4. In the **Confirm Password** box, type the password for the user a second time.
5. If the new user should have administrative privileges, select the **Administrator** check box.



Tip: When you create a user it authenticates with SSL Client Certificates. The username must match the Common Name in the certificate.

6. Click the **Create User** button.

The user saves and appears in the **Users** list.



Modify a User Account

To modify a user account:

1. On the **Users** page, select a user from the list.

The **Edit User <username>** window appears.

The screenshot shows a dialog box titled "Edit User admin". The dialog has a teal header bar with a pencil icon on the left and a close button (X) on the right. Below the header, there are three input fields: "New Password", "Confirm Password", and "Administrator" with a checkbox. At the bottom of the dialog, there are two buttons: "Update" and "Cancel".

2. Modify the properties as needed.
3. Click **Update**.

Tip: To reset user account passwords via the command line, use the following command from the **NNM** binary directory:

```
/opt/nnm/bin/nnm --users --chpasswd <username>
```




Reset a Locked Account

To reset a locked account:

1. In the command line interface, use the appropriate command for your operating system to delete the hash.lockedout file:

Operating System	Command
Linux	<code># rm /opt/nnm/var/nnm/users/<locked account name>/hash.-lockedout</code>
Windows	<code>del C:\ProgramData\Tenable\NNM\nnm\users\<locked_account_name>\hash.lockedout</code>
macOS	<code># rm /Library/NNM/var/nnm/users/<locked account name>/hash.lockedout</code>

Tip: Alternatively, a user with administrative privileges can navigate to this directory and manually delete the hash.lockedout file.

2. After deleting the hash.lockedout file, if needed, a user with administrative privileges can follow the steps under [Modify a User Account](#) to reset the user's password.



Delete a User

To delete a user:

To delete one user:

1. On the **Users** page, hover over the user you want to delete.

On the right side of the row, the ✕ button appears.

2. Click the ✕ button.

A dialog box appears confirming your selection to delete the user.

3. Click **Delete**.

The user is deleted.

To delete multiple users:

1. On the **Users** page, on the left side of the row for the user you want to delete, select the check box. Repeat this step for each user you want to delete.

2. Click **Actions > Delete Users**.

A dialog box appears confirming your selection to delete the user.

3. Click **Delete**.

The users are deleted.



Configuration Page

The **Configuration** page allows users with administrative privileges to configure Tenable Nessus Network Monitor for their local environment.

[Tenable Nessus Network Monitor Settings Section](#)

[Feed Settings Section](#)

[Cloud Settings Section](#)

[Industrial Security Settings Section](#)

[Web Proxy Settings Section](#)

[Chart Settings Section](#)

[Email Settings Section](#)

[Plugin Settings Section](#)

[Nessus Scanner Settings Section](#)



Tenable Nessus Network Monitor Settings Section

The **Tenable Nessus Network Monitor Settings** section provides options for configuring the network settings for Tenable Nessus Network Monitor. This includes what networks are monitored or excluded, how to monitor those networks, and what network interfaces Tenable Nessus Network Monitor has identified for monitoring. If your Tenable Nessus Network Monitor is licensed to run in High Performance mode, you can also [Configure Tenable Nessus Network Monitor Performance Mode](#).

Note: While you can configure many advanced settings via the command line using custom parameters, others use standard parameters. For example, while the **ACAS Classification** setting uses the custom `--add` parameter, the **Login Banner** setting does not require the `--add` parameter.

Note: The **Network Interfaces Settings** view only shows network interfaces that don't have IP addresses assigned to them. As a result, if all interfaces have assigned IP addresses, in High Performance mode, the list is empty.

Name	Description
ACAS Classification	
ACAS	<p>You can enable support for ACAS banners from the command line of the Tenable Nessus Network Monitor server service using the <code>/opt/nnm/bin/nnm --config --add "ACAS Classification" "SECRET"</code> command. SECRET may be replaced by UNCLASSIFIED, CONFIDENTIAL, TOP SECRET, or NOFORN. Once enabled, a drop-down box for the ACAS option appears in the user interface front end.</p> <p>You can disable support for ACAS banners from the command line of the Tenable Nessus Network Monitor server using the <code>/opt/nnm/bin/nnm --config --delete "ACAS Classification"</code> command from the binary directory on the server.</p>
Advanced	
Maximum Plugins Update Frequency	Specifies the maximum frequency with which plugins update.
Login Banner	Specifies a login banner.



Name	Description
	<p>Note: You can also configure login banners via the command line using the <code>/opt/nnm/bin/nnm --config "Login Banner" "NNM Banner Text"</code> command.</p>
HTTP Header Host-name Validation	<p>If you use a domain name to connect to Tenable Nessus Network Monitor, specify it in this box. Also enable Validate Host.</p> <p>To protect against malicious attacks such as header injection, Tenable Nessus Network Monitor validates that the domain name given to the browser matches your Tenable Nessus Network Monitor server. The check is case insensitive.</p>
Validate Host	<p>When enabled, specifies whether Tenable Nessus Network Monitor should validate the hostname to protect against malicious attacks.</p> <p>If you enable this setting, you must enter a value for HTTP Header Host-name Validation.</p>
Validate CSRF	<p>When enabled, Tenable Nessus Network Monitor sends anti-Cross Source Request Forgery (CSRF) tokens. This protects against malicious attacks.</p>
Session Data Size	<p>A box in which you can specify the maximum number of bytes of application layer data (e.g., FTP, HTTP, or SSH data) stored in the transport layer session cache per session. By default, the value is 3072 bytes. You can specify a minimum of 1024 bytes and a maximum of 2147483647 bytes.</p>
Enable PII Obfuscation	<p>Specifies whether or not to mask data from plugins that are expected to contain sensitive information (like Personally Identifiable Information [PII]). When enabled, the sensitive data is masked with asterisks. When disabled, the sensitive information appears in clear text in plugin output and logs. Type 0 to disable and 1 to enable the obfuscation.</p> <p>Note: By default, this option is enabled. This option cannot be disabled if your Tenable Nessus Network Monitor is connected to another application (for example, Industrial Security, Tenable Vulnerability Management, Ten-</p>



Name	Description
	<p>able Security Center).</p>
Maximum SIEM Trending Data Points	<p>Adjust this value to increase the number of SIEM Trending Data Points to take for events. SIEM events can also be increased with the Maximum Event Trending Data Points option. By default, this option is set to 10,000.</p> <p>Note: Increasing this value requires Tenable Nessus Network Monitor to allocate more memory, Tenable recommends you keep it at 10,000.</p>
Maximum Event Trending Data Points	<p>Adjust this value to increase the number of sample points to take for events. By default, this option is set to 10,000.</p> <p>Note: Increasing this value requires Tenable Nessus Network Monitor to allocate more memory, Tenable recommends you keep it at 10,000.</p>
Event Data Sample Interval In Minutes	<p>Increase this value by multiples of 5, up to the maximum of 60 (1 hour), to extend the Event Data sampling interval. The default of one minute allows you to save data for up to a week. You can also increase the number of sample points to take for events with the Maximum Event Trending Data Points and Maximum SIEM Trending Data Points options. By default, this option is set to 1.</p>
Analysis Modules	
Enable SCADA/ICS Analysis Module	<p>Enables the SCADA/ICS Analysis Module. Click the caret button to the left of the setting name to display a list of individual module detections within the module. Click on individual module detections within the list to disable/enable them. Disabling a SCADA/ICS module detection enables the legacy PASL. See the SCADA/ICS Analysis Module for more information.</p>
Enable Connection Analysis Module	<p>Enables the Connection Analysis Module. Click the caret button to the left of the setting name to display a list of individual module detections within the module. Click on individual module detections within the list to</p>



Name	Description
	disable/enable them. See the Connection Analysis Module for more information.
Enable IoT Analysis Module	When enabled, Tenable Nessus Network Monitor detects plugins in the IoT family. By default, this option is enabled.
DNS Query	
DNS Cache Life-time Analysis Module	Specifies the amount of time Tenable Nessus Network Monitor retains and stores a given host's DNS record, in seconds. By default, this option is set to 43200 (12 hours), but can be set to any value between 3600 and 172800 (48 hours).
DNS Query Time Interval	Specifies the delay between sets of DNS queries, in seconds. By default, this option is set to 5, but can be set to any value between 1 and 120.
DNS Queries per Interval	Specifies the maximum number of concurrent DNS requests made at the time of the DNS Query , in seconds. By default, this option is set to 5, but can be set to any value between 0 and 1000. Setting this value to 0 disables this feature and prevents further DNS queries from being made.
Database	
Enable Malformed Database Recovery	When enabled, allows Tenable Nessus Network Monitor to recover a malformed database.
Memory	
Sessions Cache Size	Specifies the size, in megabytes, of the session table. Adjust the session size as needed for the local network. By default, this option is set to 50.
Packet Cache Size	Specifies the maximum size, in megabytes, of the cache used to store the contents of the packets collected before processing. By default, this option is set to 128 MB with a maximum size of 512 MB. When the cache is full, any subsequent packets captured drop until space in the



Name	Description
	cache becomes available.
Monitoring	
Run in Discovery Mode	<p>Specifies whether or not Tenable Nessus Network Monitor runs in discovery mode. When enabled, Tenable Nessus Network Monitor discovers basic asset data instead of reporting vulnerabilities. This includes IP addresses, MAC addresses, hostnames, and other relevant asset data. This option is enabled by default during initial Tenable Nessus Network Monitor installation.</p> <p>Note: The Tenable Nessus Network Monitor dashboards do not display informational-level plugins. Dashboards display vulnerability plugins with a higher severity level.</p> <p>Note: If you want to link Tenable Nessus Network Monitor to an instance of Industrial Security, disable this option.</p> <p>In discovery mode, users can expect to see the following detections:</p> <ul style="list-style-type: none">• 0: Open Port.• 12: Number of Hops• 18: Generic Protocol Detection• 19: VLAN ID Detection• 20: Generic IPv6 Tunnel Traffic Detection• 113: VXLAN ID Detection• 132: Host Attribute Enumeration
Monitored Network Interfaces	<p>A list of the network devices used for sniffing packets. You can select devices individually or in multiples. Select at least one interface from the list of available devices.</p> <p>Note: High Performance mode does not support e1000 NICs as monitored</p>



Name	Description
	<p>interfaces on virtual machines. If you are running Tenable Nessus Network Monitor on a virtual machine in High Performance mode and select an e1000 monitored interface, Tenable Nessus Network Monitor automatically reverts to Standard mode.</p>
Monitored Network IP Addresses and Ranges	<p>Specifies the networks monitored. The default setting is 0.0.0.0/0, which instructs Tenable Nessus Network Monitor to monitor all IPv4 addresses. Change this to monitor only target networks; otherwise Tenable Nessus Network Monitor may quickly become overwhelmed. Separate multiple addresses by commas. When monitoring VLAN networks, you must use the syntax vlan ipaddress/subnet.</p> <p>Example: 192.0.2.0/24,2001:DB8::/64,10.2.3.0/22,vlan 192.0.2.0/16,192.168.3.123/32</p> <p>Note: The syntax is case-sensitive.</p>
Excluded Network IP Addresses and Ranges	<p>Specifies, in CIDR notation, any networks to exclude specifically from Tenable Nessus Network Monitor monitoring. This option accepts both IPv4 and IPv6 addresses. Separate multiple addresses by commas. When excluding VLAN networks, you must use the syntax vlan ipaddress/subnet. No addresses are excluded if this box is left blank.</p> <p>Note: You can exclude up to 128 CIDR entries at one time.</p> <p>Example: 192.0.2.0/24,2001:DB8::/64,10.2.3.0/22,vlan 192.0.2.0/16,192.168.3.123/32</p>
Extended Packet Filter	<p>Specifies a Berkeley Packet Filtering (BPF) expression to expand or narrow down the IP addresses being monitored. Use "or" or "and" to join your expression to the total expression for packet filtering.</p> <p>For example:</p> <ul style="list-style-type: none">• To filter vlan hierarchies two levels deep in addition to the IP address list, in the Extended Packet Filter dialog, enter: or



Name	Description
	<p>(vlan && vlan).</p> <ul style="list-style-type: none">• To require that the packets filtered by the IP address list also be two levels deep, in the Extended Packet Filter dialog, enter:and (vlan && vlan). <div data-bbox="477 485 1479 590" style="border: 1px solid #0070C0; padding: 5px;"><p>Note: These options are for packet filtering experts only. For information about available primitives, see the PCAP Filter man page.</p></div>
Enable VXLAN Traffic Analysis	Enables decoding of Virtual Extensible LAN protocol (VXLAN) traffic.
Tenable Nessus Network Monitor Proxy	
Tenable Nessus Network Monitor Restart Attempts	The number of times the Tenable Nessus Network Monitor proxy attempts to restart the Tenable Nessus Network Monitor engine in the event the engine stops running. By default, this option is set to 10, but can be set to any value between 1 and 15. Once the restart attempt limit is reached, the proxy stops trying for 30 minutes.
Tenable Nessus Network Monitor Restart Interval	The amount of time, in minutes, between Tenable Nessus Network Monitor restart attempts. By default, this option is set to 10, but can be set to any value between 1 and 3600.
Tenable Nessus Network Monitor Web Server	
Enable SSL for Web Server	<p>When selected, enables SSL protection for connections to the web server. By default, this check box is selected. Tenable does not recommend clearing the check box, as it allows the sending of unencrypted traffic between a browser and Tenable Nessus Network Monitor. You may install custom SSL certificates in the <code>/opt/nnm/var/nnm/ssl</code> directory. Restart Tenable Nessus Network Monitor after making changes to this setting.</p> <div data-bbox="477 1797 1479 1860" style="border: 1px solid #0070C0; padding: 5px;"><p>Note: Changing this option while Tenable Nessus Network Monitor is run-</p></div>



Name	Description
	<p>ning makes communication between the client and server either encrypted or unencrypted. If you select or clear the Enable SSL for Web Server check box, the Web Server automatically ends your current Tenable Nessus Network Monitor session.</p>
Minimum Password Length	Specifies the lowest number of characters a password may contain. By default, this option is set to 5, but can be set to any value between 5 and 32.
Tenable Nessus Network Monitor Web Server Address	Specifies the IPv4 or IPv6 address on which the Tenable Nessus Network Monitor web server listens. The default setting is 0.0.0.0, which instructs the web server to listen on all available IPv4 and 1Pv6 addresses. Note: Link-local addresses are not supported for IPv6 addresses.
Tenable Nessus Network Monitor Web Server Port	Specifies the Tenable Nessus Network Monitor web server-listening port. The default setting is 8835, but can be changed as appropriate for the local environment. Note: If you change the value in this box, the Web Server automatically ends your current Tenable Nessus Network Monitor session.
Tenable Nessus Network Monitor Web Server Idle Session Timeout	Specifies the number of minutes of inactivity before a web session becomes idle. By default, this option is set to 30, but can be set to any value between 5 and 60.
Enable SSL Client Certificate Authentication	When enabled, allows the web server to accept only SSL client certificates for user authentication.
Enable Debug Logging for Tenable Nessus Network Monitor Web	When enabled, allows the web server to include debug information in the logs for troubleshooting issues related to the web server. The logs become large if this option is enabled routinely.



Name	Description
Server	
Maximum User Login Attempts	Specifies the number of times a user can type an incorrect password in a 24-hour period before the user's account is locked.
Max Sessions per User	Specifies the number of concurrent sessions a user can have running at one time.
Enforce Complex Passwords	When enabled, forces the user's passwords to contain at least one uppercase character, one lowercase character, one digit, and one special character from the following: !@#\$%^&*().
Use TLS 1.2	<p>When enabled, the Tenable Nessus Network Monitor web server uses TLS 1.2 communications. By default, this option is enabled.</p> <p>Note: If you disable this option, the Tenable Nessus Network Monitor web server uses TLS 1.1, which is less secure.</p>
Disable CBC Ciphers	<p>When enabled, disables the use of CBC ciphers in TLS 1.2. By default, this option is disabled.</p> <p>Note: This setting is used in conjunction with Enable NIAP Mode. For more information, see Configure Tenable Nessus Network Monitor for NIAP Compliance.</p>
Enable Strong Encryption	<p>When enabled, forces Tenable Nessus Network Monitor to select the strongest ciphers in the TLS 1.2 communications suite. By default, this option is enabled.</p> <p>When strong encryption is enabled, the user can expect to see typical ciphers such as:</p> <ul style="list-style-type: none">• TLS_RSA_WITH_AES_128_CBC_SHA• TLS_RSA_WITH_AES_128_CBC_SHA256• TLS_RSA_WITH_AES_128_GCM_SHA256• TLS_RSA_WITH_AES_256_CBC_SHA



Name	Description
	<ul style="list-style-type: none">• TLS_RSA_WITH_AES_256_CBC_SHA256• TLS_RSA_WITH_AES_256_GCM_SHA384• TLS_RSA_WITH_CAMELLIA_128_CBC_SHA• TLS_RSA_WITH_CAMELLIA_256_CBC_SHA <p>If this option is disabled, the Tenable Nessus Network Monitor uses the following ciphers:</p> <ul style="list-style-type: none">• TLS_RSA_WITH_AES_128_CBC_SHA• TLS_RSA_WITH_AES_256_CBC_SHA <p>To configure NIAP-compliant ciphers, see Configure Tenable Nessus Network Monitor for NIAP Compliance.</p>
Plugins	
Process High Speed Plugins Only	Tenable Nessus Network Monitor is designed to find various protocols on non-standard ports. For example, Tenable Nessus Network Monitor can easily find an Apache server running on a port other than 80. However, on a high traffic network, Tenable Nessus Network Monitor can be run in High Performance mode, which allows it to focus certain plugins on specific ports. When High Performance mode is enabled and this check box is selected, any plugin that utilizes the keywords hs_dport or hs_sport are executed only on traffic traversing the specified ports.
Realtime Events	
Realtime Events File Size	Specifies the maximum amount of data from real-time events that is stored in one text file. The option must be specified in kilobytes, megabytes, or gigabytes by appending a K , M , or G , respectively, to the value.
Log Realtime Events to Realtime	When enabled, allows Tenable Nessus Network Monitor detected real-time events to be recorded to a log file in the following location:



Name	Description
Log File	<code>/opt/nnm/var/nnm/logs/realtime-logs-##.txt</code> You can configure this option via the CLI.
Enable Realtime Event Analysis	When enabled, allows Tenable Nessus Network Monitor to analyze real-time events.
Maximum Viewable Realtime Events	Specifies the maximum number of most recent events cached by the Tenable Nessus Network Monitor engine. This setting is in effect only when Realtime Event Analysis is enabled.
Maximum Realtime Log Files	Specifies the maximum number of real-time log files written to the disk.
Reports	
Report Threshold	Specifies the number of times the encryption detection algorithm executes during a session. Once the threshold is reached, the algorithm no longer executes during the session. By default, this option is set to 3 by def.
Report Lifetime	Specifies, in days, how long vulnerabilities and snapshot reports are cached. After the configured number of days is met, discovered vulnerabilities and snapshot reports are removed. This option can be set to a maximum value of 90 days. By default, this option is set to 7 and cannot be set higher than the Host Lifetime value.
Host Lifetime	Specifies, in days, how long hosts are cached. After the configured number of days is met, discovered hosts are removed. This option can be set to a maximum value of 365 days. By default, this option is set to 7 and cannot be set lower than the Report Lifetime value.
Report Frequency	Specifies, in minutes, how often Tenable Nessus Network Monitor writes a report. By default, this option is set to 15. Tenable Security Center retrieves the Tenable Nessus Network Monitor report every 15 minutes.
Knowledgebase	Specifies, in seconds, the maximum length of time that a know-



Name	Description
Lifetime	ledgebase entry remains valid after its addition. By default, this option is set to 864000.
New Asset Discovery Interval	Specifies, in days, how long Tenable Nessus Network Monitor monitors traffic before detecting new hosts. Tenable Nessus Network Monitor listens to network traffic and attempts to discover when a new host has been added. To do this, Tenable Nessus Network Monitor constantly compares a list of hosts that have generated traffic in the past to those currently generating traffic. If it finds a new host generating traffic, it issues a “new host alert” via the real-time log. For large networks, Tenable Nessus Network Monitor can be configured to run for several days to gain knowledge about which hosts are active. This prevents Tenable Nessus Network Monitor from issuing an alert for hosts that already exist. For large networks, Tenable® recommends that Tenable Nessus Network Monitor operate for at least two days before detecting new hosts. By default, this option is set to 2.
Connections to Services	When enabled, allows Tenable Nessus Network Monitor to log which clients attempt to connect to servers on the network and to what port they attempt to connect. They indicate only that an attempt to connect was made, not whether the connection was successful. Events detected by Tenable Nessus Network Monitor of this type are logged as Tenable Nessus Network Monitor internal plugin ID 2 .
Show Connections	When enabled, instructs Tenable Nessus Network Monitor to record clients in the focus network that attempt to connect to a server IP address and port and receive a positive response. The record contains the client IP address, the server IP address, and the server port that the client attempted to connect to. For example, if four different hosts within the focus network attempt to connect with a server IP over port 80 and received a positive response, then a list of those hosts are reported under Tenable Nessus Network Monitor internal plugin ID 3 and port 80.
Known Hosts File	Note: You can only configure this feature via the command-line interface.



Name	Description
	<p>A configuration parameter in which you can type the location of the known-hosts.txt file. Manually create the Known Hosts file.</p> <p>This feature supports a single row for each IP (IPv4 or IPv6). Hyphenated ranges and CIDR notation are not supported. New host alerts no longer appear for the hosts listed in this file.</p> <div data-bbox="479 531 1479 688" style="border: 1px solid #0070C0; padding: 5px;"><p>Note: Blank rows are ignored, and invalid entries are noted in the Tenable Nessus Network Monitor log file. If you make any changes to the Known Hosts file, you must restart Tenable Nessus Network Monitor.</p></div>
Security Options	
Enable FIPS Mode	<p>When enabled, Tenable Nessus Network Monitor uses OpenSSL 3.0 FIPS module security features. The OpenSSL 3.0 FIPS module is a set of encryption modules satisfying the requirements of the FIPS 140-2 standard defined by the National Institute of Standards and Technology (NIST).</p> <div data-bbox="479 1060 1479 1176" style="border: 1px solid #0070C0; padding: 5px;"><p>Note: If you use the FIPS module, you may need to restart Tenable Nessus Network Monitor a few times.</p></div>
Enable National Information Assurance Partnership (NIAP) Mode	<p>When enabled, Tenable Nessus Network Monitor uses NIAP ciphers in compliance with NIAP standards.</p> <p>If you enable this setting, then you must also enable Enable FIPS Mode.</p>
NIAP Mode Disabled Due to Upgrade	<p>When enabled, Tenable Nessus Network Monitor does not use FIPS or NIAP security features.</p>
Session Analysis	
Encrypted Sessions Dependency Plugins	<p>Specifies the Plugin IDs, separated by commas, used to detect encrypted traffic.</p>



Name	Description
Encrypted Sessions Excluded Network Ranges	Specifies the IPv4 and IPv6 addresses and ports, in CIDR notation, excluded from monitoring for encrypted traffic. Example: 192.0.2.0/24,2001:DB8::/64,10.2.3.0/22,vlan 192.0.2.0/16,192.168.3.123/32
Interactive Sessions Dependency Plugins	Specifies the plugin IDs, separated by commas, used to detect interactive sessions.
Interactive Sessions Excluded Network Ranges	Specifies the IPv4 and IPv6 addresses and ports, in CIDR notation, excluded from monitoring for interactive sessions. Example: 192.0.2.0/24,2001:DB8::/64,10.2.3.0/22,vlan 192.0.2.0/16,192.168.3.123/32

SIEM Processing Options

Note: SIEM analysis features are only available for RH/CentOS 7 and RH/CentOS 8.

Enable SIEM Assets Discovery	When selected, allows Tenable Nessus Network Monitor to discover assets through SIEM analysis. For more information, see SIEM Analysis Section .
Enable SIEM User Account Activity	When selected, allows Tenable Nessus Network Monitor to detect user account activity through SIEM analysis. For more information, see SIEM Analysis Section .
Enable SIEM Software Detection	When selected, allows Tenable Nessus Network Monitor to detect software events through SIEM analysis. For more information, see SIEM Analysis Section .
Enable SIEM Service Modification	When selected, allows Tenable Nessus Network Monitor to detect service modification events through SIEM analysis. For more information, see SIEM Analysis Section .
SIEM Polling Interval	The interval, in minutes, after which Tenable Nessus Network Monitor updates its status with the SIEM servers and asks for a list of



Name	Description
	jobs. Options are in the range of 5-10 minutes.
Maximum SIEM Trending Data Points	<p>Adjust this value to increase the number of SIEM Trending Data Points to take for events. SIEM events can also be increased with the Maximum Event Trending Data Points option. By default, this option is set to 10,000.</p> <div data-bbox="479 533 1477 648"><p>Note: Increasing this value requires Tenable Nessus Network Monitor to allocate more memory, Tenable recommends you keep it at 10,000.</p></div>
SIEM Servers	
SIEM Servers List	<div data-bbox="479 747 1477 863"><p>Note: SIEM analysis features are only available for RH/CentOS 7 and RH/CentOS 8.</p></div> <p>Lists the servers used to track SIEM-related events. The charts shown in the SIEM Analysis section pull data from these servers. This section provides three options:</p> <ul style="list-style-type: none">• Add - Add a new SIEM server setting. Enter the following information:<ul style="list-style-type: none">• IP - The server IP address.• Port (TCP) - The server IP port number.• SIEM Type - The server's SIEM type (Splunk).• User - The username that grants server access.• Password - The password that grants server access.• Edit - Edit the SIEM server settings listed above.• Delete - Delete the selected SIEM server and all related SIEM queries. <div data-bbox="479 1738 1477 1833"><p>Note: SIEM server entries are displayed as User@IP_Address:Port (e.g., admin@1.2.3.4:8089). The combination of these three parameters is</p></div>



Name	Description
	<p data-bbox="477 239 1479 310">unique; entries with the same three parameters are rejected.</p> <p data-bbox="477 338 1479 451">Note: Tenable recommends that you only use trusted self-signed certificates for Splunk instances used with Tenable Nessus Network Monitor.</p>
Syslog	
Realtime Syslog Server List	<p data-bbox="477 558 1479 743">Specifies the IPv4 or IPv6 address and port of a Syslog server to receive real-time events from Tenable Nessus Network Monitor. Click Add to save the address. A local Syslog daemon is not required. Syslog items can be specified to Standard or CEF formats and UDP or TCP protocols.</p> <p data-bbox="477 779 1406 814">Example: 192.0.2.12:4567,10.10.10.10:514,[2001:DB8::23B4]:514</p>
Vulnerability Syslog Server List	<p data-bbox="477 852 1479 1087">Specifies the IPv4 or IPv6 address and port of a Syslog server to receive vulnerability data from Tenable Nessus Network Monitor. Click Add to save the address. A local Syslog daemon is not required. You can specify Syslog items to Standard or CEF formats and UDP or TCP protocols.</p> <p data-bbox="477 1123 1406 1159">Example: 192.0.2.12:4567,10.10.10.10:514,[2001:DB8::23B4]:514</p> <p data-bbox="477 1192 1479 1339">Note: While Tenable Nessus Network Monitor may display multiple log events related to one connection, it sends only a single event to the remote Syslog server(s).</p>



Configure Tenable Nessus Network Monitor Performance Mode

Before you begin:

This option appears only when Tenable Nessus Network Monitor is licensed to run in High Performance mode and the machine running Tenable Nessus Network Monitor meets the [hardware](#) and [software](#) requirements for High Performance mode. By default, all instances of Tenable Nessus Network Monitor run in Standard mode.

Tenable Nessus Network Monitor must restart when switching between performance modes.

To configure performance mode:

1. Click **Configuration > Tenable Nessus Network Monitor Settings**.
2. Under the **Performance Mode** heading, click the **Enable High Performance Mode** box to toggle between **Yes** and **No**. If you select **Yes**, continue to step 3. If you select **No**, continue to step 4.

The screenshot shows a dialog box titled "Performance Mode". It contains two settings: "Enable High Performance Mode" with a toggle switch currently set to "Yes", and "Number of Worker Cores" with a dropdown menu currently set to "1". At the bottom of the dialog are two buttons: "Update" (highlighted in blue) and "Cancel".

3. In the **Number of Worker Cores** drop-down box, select the appropriate number of worker cores.

Note: This option cannot be changed when Tenable Nessus Network Monitor is already running in High Performance mode.

4. Click the **Update** button.

A dialog box appears confirming your selection to change the performance mode.

5. Click the **Confirm** button.



Tenable Nessus Network Monitor restarts and the login screen appears. When the Tenable Nessus Network Monitor server resumes, a notification appears indicating whether the configuration change was successful.

Note: Tenable Nessus Network Monitor may use a different number of cores than the number you select. Based on system constraints and your selection, Tenable Nessus Network Monitor selects the closest number of worker cores that it can feasibly support.

6. Log in to Tenable Nessus Network Monitor.

The performance mode updates.



Feed Settings Section

The **Feed Settings** section allows you to:

Name	Description
Register Offline check box	A check box that allows offline registration of Tenable Nessus Network Monitor.
Activation Code box	Updates the activation code. The Activation Code only needs to be updated when it expires.
Fetch Plugins From drop-down box	A drop-down box from which you can specify where you wish to fetch plugins. Click Update to fetch the plugins.
Offline Plugin Archive	Uploads plugins to perform offline updates. Choose File to select the file to upload, then click Upload Archive to upload the archive.
Host Address box	A box in which you can specify a custom plugin feed host. Click Update to save the host.


Offline Update

The **Offline Update** allows a user with administrative privileges to manually update plugins when the Tenable Nessus Network Monitor host cannot connect to the Internet.

1. [Download the plugin update archive](#) from Tenable®.
2. Click **Choose File**.
3. Select the archive tarball to upload.
4. Click the **Upload Archive** button to send the file to the Tenable Nessus Network Monitor host.
5. Click the **Upload Archive** button again to update the plugins.
6. If a new client is part of the update, you must refresh the web browser to see the updated client.

The **Custom Plugin Feed** host is an alternate feed host. These are typically hosted on a local network to provide custom Tenable Nessus Network Monitor plugins.



When running Standalone Tenable Nessus Network Monitor or Tenable Nessus Network Monitor in High Performance mode as **Managed by Tenable Security Center** or **Managed by Tenable Vulnerability Management**, you must type an Activation Code before clicking the **Update** button. The  button schedules a plugin update when Tenable Nessus Network Monitor is running in **Standalone** mode. Additionally, when registering Tenable Nessus Network Monitor in **Offline** mode, you need the Activation Code to obtain the Activation Key.




Download New Vulnerability Plugins

Before You Begin

When Tenable Nessus Network Monitor is registered in **Standalone** mode using an Activation code, plugins are updated automatically every 24 hours after the service is started.

If Tenable Security Center or Tenable Vulnerability Management is used to manage Tenable Nessus Network Monitor, new plugins for Tenable Nessus Network Monitor are automatically sent at scheduled intervals.

To manually download new vulnerability plugins:

1. Click **Configuration > Feed Settings**.
2. Next to the **Fetch Plugins From** drop-down box, click the  button.

Tip: The plugins can also be updated by using the following command:
/opt/nnm/bin/nnm --update-plugins



Updating the Tenable Nessus Network Monitor Management Interface

On occasion, the Tenable Nessus Network Monitor management interface must be updated to provide new or updated features.

To manually update the plugins:

1. Download the latest plugins using the URL created during the offline registration process.
2. Log in to the Tenable Nessus Network Monitor interface as a user with administrative privileges.
3. Click **Configuration > Feed Settings**.
4. In the **Offline Update** section, click **Choose File**.

A dialog box appears.

5. Select the archive file to upload.
6. Click **Upload Archive** to send the file to the Tenable Nessus Network Monitor host, which updates the plugins.
7. Stop Tenable Nessus Network Monitor on the host.
8. Restart Tenable Nessus Network Monitor on the host.

The new interface is available for use.

Cloud Settings Section

The **Cloud Settings** section provides options for configuring Tenable Nessus Network Monitor to communicate with Tenable Vulnerability Management.

Cloud Settings

Cloud Host:

Cloud Port:

Cloud Key:

Polling Frequency:

NNM Name:

Name	Description
Cloud Host	The domain name or IP address of the Tenable Vulnerability Management server: sensor.cloud.tenable.com .
Cloud Port	The port of the Tenable Vulnerability Management server: 443 .
Cloud Key	The Tenable Vulnerability Management key used to link this instance of Tenable Nessus Network Monitor to a Tenable Vulnerability Management account. See Link a Sensor in the Tenable Vulnerability Management User Guide for more information.
Polling Frequency	The frequency, in seconds, with which Tenable Nessus Network Monitor updates its status with Tenable Vulnerability Management and



Name	Description
	asks for a list of jobs.
NNM Name	The unique name used to identify this instance of Tenable Nessus Network Monitor in Tenable Vulnerability Management.

By default, Tenable Vulnerability Management pulls data from the Tenable Nessus Network Monitor scanner every 60 minutes. This is determined by the **Report Frequency** setting in Tenable Vulnerability Management. Once the linked Tenable Nessus Network Monitor scanner is added to Tenable Vulnerability Management, a scan is automatically created and results are collected from Tenable Nessus Network Monitor. If the **Report Frequency** setting is changed, the scans adjust automatically.



Industrial Security Settings Section

Industrial Security is end-of-life (EOL). For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle [Matrix](#) and [Policy](#).

The **Industrial Security Settings** section provides options for configuring Industrial Security with Tenable Nessus Network Monitor. For more information, see [Configure Tenable Nessus Network Monitor for use with Industrial Security](#).

Note: To use Tenable Nessus Network Monitor with Industrial Security, disable the discovery mode option. For more information, see [Tenable Nessus Network Monitor Settings Section](#).

- ⚙️ NNM Settings
- 📡 Feed Settings
- ☁️ Cloud Settings
- 🔑 Industrial Security Settings
- ⚙️ Web Proxy Settings
- 📊 Chart Settings
- ✉️ Email Settings
- 🔗 Plugin Settings
- 🔍 Nessus Scanner Settings

Industrial Security Settings

Industrial Security Host	<input type="text"/>
Industrial Security Port	<input type="text" value="8837"/>
Industrial Security Key	<input type="text"/>
Polling Frequency	<input type="text" value="30"/>
NNM Name	<input type="text"/>

Name	Description
Industrial Security Host	The domain name or IP address of the Industrial Security server.



Name	Description
Industrial Security Port	The port of the Industrial Security server.
Industrial Security Key	The key used to link this instance of Tenable Nessus Network Monitor to a Industrial Security account.
Polling Frequency	The frequency, in seconds, with which Tenable Nessus Network Monitor updates its status with Industrial Security and asks for a list of jobs.
Tenable Nessus Network Monitor Name	The unique name used to identify this instance of Tenable Nessus Network Monitor on Industrial Security.

Web Proxy Settings Section

The **Web Proxy Settings** section configures the settings for a web proxy if one is needed for plugin updates. These settings include the proxy host IP address, port, username, password, and, if a custom agent string is needed, a user-agent box.

[NNM Settings](#)

[Feed Settings](#)

[Cloud Settings](#)

[Industrial Security Settings](#)

Web Proxy Settings

[Chart Settings](#)

[Email Settings](#)

[Plugin Settings](#)

[Nessus Scanner Settings](#)

Web Proxy For Plugin Updates

Host Address

Port

Username

Password

User-Agent String

Web Proxy Method

Name	Description
Host Address	The host address of the web proxy server.
Port	The port of the web proxy server.
Username	The username for the web proxy server.
Password	The password for the web proxy server.
User-Agent String	The user agent for the web proxy server, if your proxy requires a preset user agent.
Web Proxy Method	The authentication method Tenable Nessus Network Monitor uses to connect to the web proxy server. Type one of the following values:



Note: For the *auto* and *basic* methods, the web proxy **Username** and **Password** values are required for Tenable Nessus Network Monitor to engage with the proxy.

- *auto* - Tenable Nessus Network Monitor detects and uses the method available for the web proxy.
- *basic* - Tenable Nessus Network Monitor uses basic authentication, which encodes the username and password with Base64.
- *digest* - Tenable Nessus Network Monitor uses HTTP Digest authentication, which uses a hash function to encrypt the username and password.
- *ntlm* - Tenable Nessus Network Monitor uses Microsoft NTLM user authentication in a Windows domain.

Note: NTLM is deprecated by Microsoft. This authentication method is not recommended and should be used only for compatibility with older configurations.



Chart Settings Section

The **Chart Settings** section displays all charts available, provides options for [creating and configuring charts](#), and allows the user to add or remove charts in the **Dashboards** section.

In the **Chart Settings** section you can view:

- The chart **Type**.
- The **Name** of the chart.
- A **Description** of the chart.
- The chart's **Dashboard Family**.
- A toggle that determines if the chart appears in the Dashboard. Click the option to toggle between **Yes** and **No**.

Click on a chart to edit the chart.

The screenshot shows the 'Chart Settings' section of a management console. On the left is a sidebar with navigation links: NNM Settings, Feed Settings, Cloud Settings, Industrial Security Settings, Web Proxy Settings, Chart Settings (highlighted), Email Settings, Plugin Settings, and Nessus Scanner Settings. The main area is titled 'Chart Settings' and contains a table with the following columns: a checkbox, Type, Name, Description, Dashboard Family, and View in Dashboard. The 'View in Dashboard' column contains a 'Yes' toggle switch for each row.

<input type="checkbox"/>	Type	Name	Description	Dashboard Family	View in Dashboard
<input type="checkbox"/>		Distribution by Operating System	Distribution by operating system	Top N	Yes
<input type="checkbox"/>		Distribution of Mobile Applications by App...	Distribution of mobile applications by appl...	Top N	Yes
<input type="checkbox"/>		Distribution of Mobile Devices by Operatin...	Distribution of mobile devices by operatin...	Top N	Yes
<input type="checkbox"/>		SCADA Host Distribution by Protocol	Distribution of SCADA hosts by protocol	SCADA	Yes
<input type="checkbox"/>		SCADA Host Distribution by System Type	Distribution of SCADA hosts by system type	SCADA	Yes
<input type="checkbox"/>		SCADA Vulnerability Distribution by Severity	Distribution of SCADA vulnerabilities by s...	SCADA	Yes
<input type="checkbox"/>		Top 10 Hosts	Chart of top 10 monitored hosts by vulner...	Top N	Yes
<input type="checkbox"/>		Top 10 Mobile Devices	Chart of top 10 monitored monitored devi...	Top N	Yes
<input type="checkbox"/>		Top 10 Mobile Devices by Hardware	Top 10 mobile devices by hardware	Top N	Yes
<input type="checkbox"/>		Top 10 SCADA Hosts	Chart of top 10 monitored SCADA hosts b...	SCADA	Yes
<input type="checkbox"/>		Top 10 Talkers	Chart of top 10 talkers	Top N	Yes
<input type="checkbox"/>		Top 10 Vulnerabilities	Chart of top 10 vulnerabilities by severity	Top N	Yes
<input type="checkbox"/>		Top 5 Applications	Chart of top 5 applications by severity	Top N	Yes



Create a Custom Chart

To create a custom chart:

1. Click **Configuration > Chart Settings > Create Chart**.

The **Create Chart** window appears.

+ Create Chart [Close]

Name: Custom Pie Chart

Description: Example pie chart depicting the top 10 machines running BitTorrent Clients.

Current Chart Query: Choose a Chart Type below to begin building your chart query.

Chart Type: [Pie Chart Icon] [Bar Chart Icon]

Dashboard Family: Category

[Create Chart] [Cancel]

2. In the **Name** box, type a name for the chart.

Note: In this example, we are creating a chart that displays the top vulnerabilities for machines reporting associated BitTorrent activity.

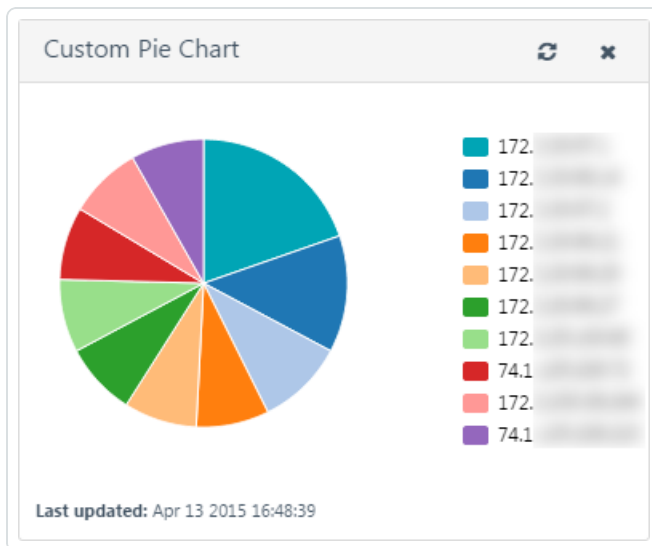
3. In the **Description** box, type a description for the chart.
4. In the **Chart Type** section, select the type of chart you want to create.
5. In the **Dashboard Family** section, type a numeric value between 1 and 20 that represents the number of items returned for this chart.
6. Click **Top** to add the value to the **Current Chart Query** section.



7. In the **Category** section, select a chart category. The selected category determines the type of items displayed on the chart, such as hosts, vulnerabilities, applications, operating systems, or connections.
8. In the **Filters** section, configure the options by which you want to filter the results.

Note: In this example, we are creating a filter based on the Plugin ID 3920. This triggers when BitTorrent client activity is detected.

9. Click the **+** button to apply the rule to the chart.
10. In the **Viewable** section, select whether you want the chart to appear on the main dashboard.
11. Click the **Create Chart** button. The chart appears in the **Dashboards** section of the **Monitoring** page.





Delete a Chart

Note: You cannot delete default charts.

To delete a chart:

To delete one chart:

1. Click **Configuration > Chart Settings**.
2. Hover over the chart you want to delete.
3. On the right side of the row, click the **✕** button.

A dialog box appears confirming your selection to delete the chart.

4. Click **Delete**.

The chart is deleted.

To delete multiple charts:

1. Click **Configuration > Chart Settings**.
2. On the left side of the row for the chart you want to delete, select the check box.
3. Repeat step 2 for each chart you want to delete.
4. Click **Actions > Delete Charts**.

A dialog box appears confirming your selection to delete the charts.

5. Click **Delete**.

The charts are deleted.



Email Settings Section

The **Email Settings** section allows you to [Create an Email Notification](#) for Tenable Nessus Network Monitor. You can specify the recipients of the email notifications, what charts appear in email notifications, and the time and frequency with which email notifications are sent. To send a report immediately, in the **Email Settings** section, hover over an existing email notification and click the paper airplane icon.

The screenshot shows the 'Email Settings' section. On the left, a sidebar lists settings categories: NNM Settings, Feed Settings, Cloud Settings, Industrial Security Settings, Web Proxy Settings, Chart Settings, Email Settings (selected), Plugin Settings, and Nessus Scanner Settings. The main area is titled 'Email Settings' and features a 'Setting Type' dropdown menu set to 'Email Notifications'. Below this is a table with the following data:

<input type="checkbox"/>	Name	Description	Frequency	Recipients
<input type="checkbox"/>	Distribution By Operating Syst...		Weekly	nnmuser@mydomain.com
<input type="checkbox"/>	Top 10 Vulnerability Notification		Once	nnmuser@mydomain.com

When you select **SMTP Server** in the **Setting Type** drop-down box, the following options for configuring the SMTP server appear:

Name	Description
Host	The host or IP of the SMTP server (e.g., smtp.example.com).
Port	The port of the SMTP server (e.g., 25).
From	The name that appears in the "From" line of the email report.
Tenable Nessus Network Monitor Location	The IP address or hostname of your Tenable Nessus Network Monitor server. This works only if the user that receives the email report can reach the Tenable Nessus Network Monitor host.
Auth Method	The method by which the SMTP server is authenticated. Supported methods are None , Plain , NTLM , Login , and CRAM-MD5 .

Note: If this option is set to **None**, the **Username** and **Password** boxes are hid-



Name	Description
	<input data-bbox="428 239 1458 315" type="text" value="den."/>
Username	The username used to authenticate to the SMTP server.
Password	The password associated with the username, provided that a password is required by the SMTP server.



Create an Email Notification

To create an email notification:

1. Click **Email Settings > Create Email Notification**.

The **Create Email Notification** window appears.

2. In the **Name** box, type a name for the email notification.
3. In the **Description** box, type a description for the email notification.
4. Click **Next Step**.

The **Add Charts** screen appears.

5. Select the check boxes that correspond to the charts you want to add to the email notification.
6. Reorder the charts by clicking and dragging the appropriate **≡➔** button.
7. Click **Next Step**.

The **Schedule Email Notification** screen appears.

8. Select the frequency, date, and time at which you want the email notification to be sent. Depending on the option you select in the **Frequency** box, the following additional options appear:

Frequency	Options
Once	None
Hourly	Repeat Every - a drop-down box that includes options from 1 to 20 hours.
Daily	Repeat Every - a drop-down box that includes options from 1 to 20 days.
Weekly	Repeat Every - a drop-down box that includes options from 1 to 20 weeks. Repeat On - a multi-selectable list of the days of the week.



Frequency	Options
Monthly	Repeat Every - a drop-down box that includes options from 1 to 20 months. Repeat By - a drop-down box that includes the options Week of Month and Day of Month.
Yearly	Repeat Every - a drop-down box that includes options from 1 to 20 years.

The **Summary** box updates automatically depending on your selection.

9. Click **Next Step**.

The **Add Recipients** screen appears.

10. In the **Recipients** box, type an email address and click the **+** button until you have added all desired recipients.
11. Click **Next Step**.

The **Review Email Notification** screen appears, which displays a summary of your email notification configuration.

12. Review the notification details.
13. Click **Finish**.



Delete an Email Notification

To delete an email notification:

To delete one email notification:

1. Click **Configuration > Email Settings**.
2. Hover over the email notification you want to delete.
3. On the right side of the row, click the **x** button.

A dialog box appears confirming your selection to delete the email notification.

4. Click the **Delete** button.

The email notification is deleted and the corresponding notifications are no longer sent.

To delete multiple email notifications:

1. Click **Configuration > Email Settings** section.
2. On the left side of the row for the email notification you want to delete, select the check box.
3. Repeat step 2 for each email notification you want to delete.
4. Click **Actions > Delete Notifications**.

A dialog box appears confirming your selection to delete the email notifications.

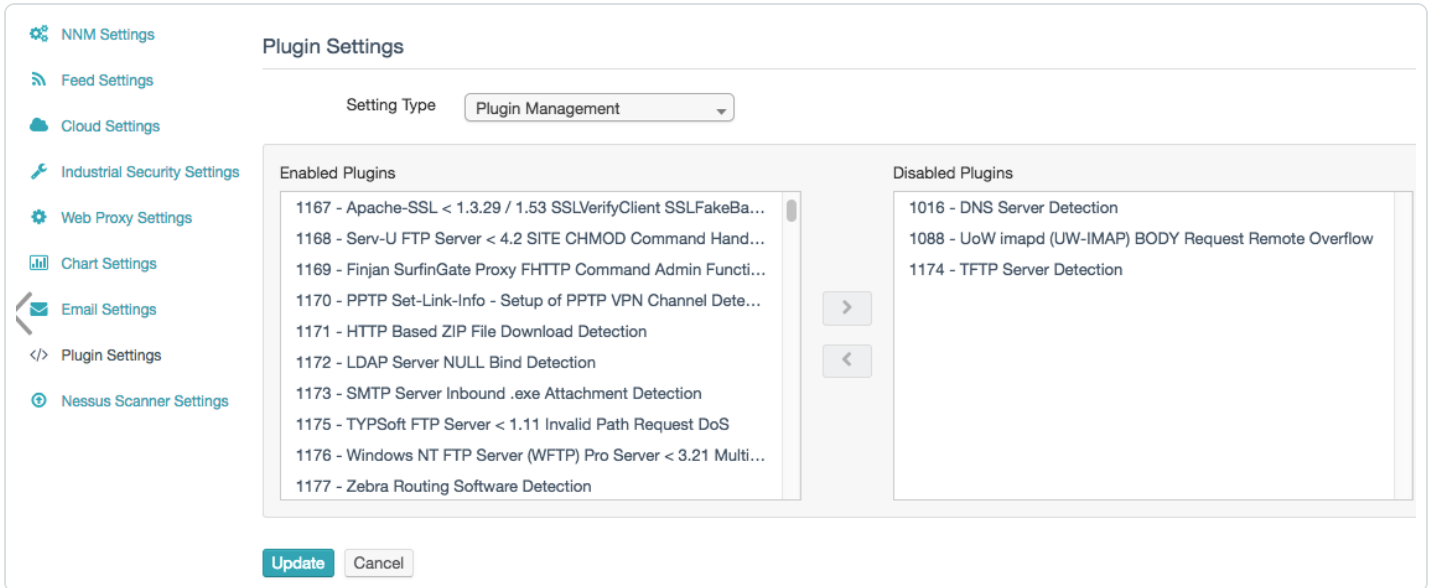
5. Click the **Delete** button.

The email notifications are deleted and the corresponding notifications are no longer sent.



Plugin Settings Section

The **Plugin Settings** section allows you to create custom, passive plugins, enable/disable existing plugins and PASLs, and modify the SIEM core queries.



The **Plugin Settings** section contains the following subsections:

- **Plugin Management** - Provides a list of enabled and disabled plugins, respectively, the options to move plugins between those lists, and the option to delete custom plugins.
- **PASL Management** - Provides a list of enabled and disabled PASLs, respectively, and the options to move PASLs between those lists.
- **SIEM Plugin Management** - Shows options for managing plugins related to SIEM analysis.

Note: SIEM analysis features are only available for RH/CentOS 7 and RH/CentOS 8.

The following table provides a brief summary of each SIEM plugin setting:

SIEM Plugin Option	Purpose
Key Name	The SIEM event category for events collected from a Windows or Linux system.



SIEM Plugin Option	Purpose
Plugin IDs	The plugin IDs associated with the selected SIEM event category/ Key Name .
SIEM Server	The SIEM server related to the plugin. The options for this box are configured in the SIEM Servers section of the Tenable Nessus Network Monitor Settings Section .
Query Prefix	(Optional) The custom query prefix for additional query functionality.
Core Query	The system-generated query related to the selected Key Name . This query is not configurable.
Query Suffix	(Optional) The custom query suffix for additional query functionality.

- **Create Custom Plugin** - Shows options for creating custom plugins and creating new plugin fields.

The following table provides a brief summary of each custom plugin option:

Custom Plugin Option	Purpose
ID	The unique numeric ID of the plugin.
Name	The name of the plugin. The plugin name should start with the vendor name.
Description	The full text description of the vulnerability.
Synopsis	A brief description of the plugin or vulnerability.
Solution	Remediation information for the vulnerability.
See Also	External references to additional information regarding the vulnerability.



Custom Plugin Option	Purpose
Risk	Info, Low, Medium, High, or Critical risk factor.
Plugin Output	Displays dynamic data in Tenable Nessus Network Monitor plugin reports.
Family	The family to which the plugin belongs.
Dependency	Other dependencies required to trigger the custom plugin.
NoPlugin	Prevents a plugin from being evaluated if another plugin has already matched. For example, it may make sense to write a plugin that looks for a specific anonymous FTP vulnerability, but to disable it if another plugin that checked for anonymous FTP had already failed.
No Output	For plugins that are written specifically to be used as part of a dependency with another plugin. When enabled, this keyword causes Tenable Nessus Network Monitor not to report anything for any plugin.
Client Issue	Indicates the vulnerability is located on the client side.
Plugin Type	Vuln, realtime, or realtimeonly plugin type.
cve	The CVE reference.
bid	The Bugtraq ID (BID) reference.
osvdb	The external reference (e.g., OSVDB, Secunie, MS Advisory).
nid	To track compatibility with the Tenable Nessus vulnerability scanner, Tenable® associates Tenable Nessus Network Monitor vulnerability checks with relevant Tenable Nessus vulnerability checks. Multiple Tenable Nessus IDs can be listed under one nid entry such as nid=10222,10223 .
cpe	Filters the result of discovered vulnerabilities based on their



Custom Plugin Option	Purpose
	CPE identifier.
Match	This keyword specifies a set of one or more simple ASCII patterns that must be present in order for the more complex pattern analysis to take place. The <code>match</code> keyword gives Tenable Nessus Network Monitor significant performance and functionality.
Regex	Specifies a complex regular expression search rule applied to the network session.
Revision	The revision number associated with custom plugin.
Raw Text Preview	<p>A preview of the custom plugin in raw text. An example of a custom plugin created to find a IMAP Banner of Tenable Rocks is:</p> <pre data-bbox="526 905 1458 1325">id=79000 name=IMAP Banner description=An IMAP server is running on this port. Its banner is Tenable Rocks risk=NONE match=OK match=IMAP match=server ready regex=^.*OK.*IMAP.*Tenable Rocks</pre>



Add a Plugin Field

1. Click **Configuration > Plugin Settings > Setting Type > Create Custom Plugin > Add Plugin Field**.

The **Add Plugin Field** window appears.

+ Add Plugin Field ×

Create New Field

Name

Value Type

Allow duplicates

Replace XML special characters

Add

2. In the **Name** box, type a name for the plugin.
3. From the **Value Type** drop-down box, select a value type for the plugin.
4. If you wish to allow duplicates of this plugin, select the **Allow Duplicates** check box.
5. If you wish to replace XML special characters, select the **Replace XML Special Characters** check box.
6. Click **Add**.

The new plugin fields appear below the **No Output** check box.



Delete a Custom Plugin

1. Click **Configuration > Plugin Settings**.
2. Select the custom plugin(s) that you want to delete.
3. Click **Actions > Delete Custom Plugins**.

A dialog box appears confirming your selection to delete the custom plugins. You can delete only user-created plugins.

4. Click **Delete**.

The custom plugins are deleted.



Nessus Scanner Settings Section

The **Nessus Scanner Settings** section provides a list of the available Tenable Nessus 6.4+ scanners and the ability to add, edit, or remove a Tenable Nessus scanner.

Scanner Host	Scanner Port
172...	8834

Note: Tenable Nessus Professional 7 is not supported.

Each Tenable Nessus scanner must be configured with the following parameters:

Name	Description
Scanner Host	The domain name or IP address of the Tenable Nessus server.
Scanner Port	The port of the Tenable Nessus server.
Access Key	The first half of a Tenable Nessus API Key, which is used to authenticate with the Tenable Nessus REST API.
Secret Key	The second half of a Tenable Nessus API Key, which is used to authenticate with the Tenable Nessus REST API.

Note: For details on how to obtain an API Key (Access Key and Secret Key), refer to the [Tenable Nessus user guide](#).



Add a Tenable Nessus Scanner

To add a Tenable Nessus Scanner:

1. Click **Configuration > Nessus Scanner Settings > Add Nessus Scanner**.

The **Add Nessus Scanner** window appears.

2. In the **Scanner Host** box, type the domain name or IP address of the Tenable Nessus server.
3. In the **Scanner Port** box, type the port of the Tenable Nessus server.
4. In the **Access Key** box, type the first half of a Tenable Nessus API Key, which is used to authenticate with the Tenable Nessus REST API.
5. In the **Secret Key** box, type the second half of a Tenable Nessus API Key, which is used to authenticate with the Tenable Nessus REST API.
6. Click the **Add Nessus Scanner** button.

The Tenable Nessus scanner appears in the **Nessus Scanner Settings** section.



Delete a Tenable Nessus Scanner

To delete a Tenable Nessus scanner:

To delete one Tenable Nessus Scanner:

1. Click **Configuration > Nessus Scanner Settings**.
2. Hover over the scanner you want to delete.
3. Click the **x** button.

A dialog box appears confirming your selection to delete the scanner.

4. Click **Delete**.

The scanner is deleted.

To delete multiple Tenable Nessus Scanners:

1. Click **Configuration > Nessus Scanner Settings** section.
2. On the left side of the row for the scanner you want to delete, select the check box
3. Repeat step 2 for each scanner you want to delete.
4. Click **Actions > Delete Nessus Scanners**.

A dialog box appears confirming your selection to delete the scanners.

5. Click **Delete**.

The scanners are deleted.



Additional Resources

This section describes the following information about Tenable Nessus Network Monitor that is not included in the **Features** and **How To** sections:

- [Command Line Operations](#)
- [Unknown or Customized Ports](#)
- [Real-Time Traffic Analysis Configuration Theory](#)
- [Modules](#)
- [Internal Tenable Nessus Network Monitor Plugin IDs](#)
- [Tenable Nessus Network Monitor Plugins](#)
- [Working with Tenable Security Center](#)
- [Syslog Message Formats](#)
- [Custom SSL Certificates](#)
- [Configure Tenable Nessus Network Monitor for Certificates](#)

For more Tenable Nessus Network Monitor deployment information, see the [Tenable Nessus Network Monitor Deployment Guide](#).



Command Line Operations

The Tenable Nessus Network Monitor engine provides many options to update and configure Tenable Nessus Network Monitor from the command line in Linux, Windows, and macOS. All command lines should be run by users with root or administrative privileges.

- [Common Command Line Operations](#)
- [Linux Command Line Operations](#)
- [Windows Command Line Operations](#)
- [macOS Command Line Operations](#)



Common Command Line Operations

Tenable Nessus Network Monitor can be run from the command line to update plugins, perform configuration tasks, and analyze Pcap files to generate a report file for use with Tenable Security Center or other programs. Running the Tenable Nessus Network Monitor binary with the `-h` option displays a list of available options.

Note: You must stop Tenable Nessus Network Monitor before running command line operations.

Tenable Nessus Network Monitor Binary Locations

The Tenable Nessus Network Monitor binary for Linux can be found in the following location:

```
# /opt/nnm/bin/nnm
```

The Tenable Nessus Network Monitor binary for Windows can be found in the following location:

```
C:\Program Files\Tenable\NNM\nnm.exe
```

The Tenable Nessus Network Monitor binary for macOS can be found in the following location:

```
# /Library/NNM/bin/nnm
```

Tenable Nessus Network Monitor Command Line Options

Note: While you can configure many advanced settings via the command line using custom parameters, others use standard parameters. For example, while the **ACAS Classification** setting uses the custom `--add` parameter, the **Login Banner** setting does not require the `--add` parameter.

Option	Purpose
<code>-a <activation code></code>	<p>Type the Activation Code to activate Tenable Nessus Network Monitor in standalone mode to enable plugin updates and monitoring functions.</p> <p>If your Tenable Nessus Network Monitor system is managed by Tenable Security Center and is running in Standard mode, you can use the following command: <code>-a SecurityCenter</code></p> <p>If your Tenable Nessus Network Monitor system is managed by Tenable Security Center and is running in High Performance mode, you can</p>



Option	Purpose
	<p>use the following command: -a SecurityCenter <activation code></p> <p>If your Tenable Nessus Network Monitor system is managed by Tenable Vulnerability Management and is running in Standard mode, you can use the following command: -a Cloud</p> <p>If your Tenable Nessus Network Monitor system is managed by Tenable Vulnerability Management and is running in High Performance mode, you can use the following command: -a Cloud <activation code></p> <div data-bbox="464 751 1458 907" style="border: 1px solid #0070C0; padding: 5px;"><p>Before running the -a command for Tenable Nessus Network Monitor that is managed by Tenable Vulnerability Management, you should first configure the Cloud Host, Cloud Port, Cloud Key, and NNM Name parameters.</p></div>
<pre>--config --add "custom_ parameter name" "parameter value"</pre>	Add a custom configuration parameter for Tenable Nessus Network Monitor or an Tenable Nessus Network Monitor Proxy. The double quote characters are required, although single quotes may be used when special characters are required.
<pre>--config -- delete "custom_ parameter name"</pre>	The delete command may be used to remove custom configuration parameters.
<pre>--config -- list</pre>	Lists the current Tenable Nessus Network Monitor and Tenable Nessus Network Monitor Proxy configuration parameters. Parameter values are listed to the left of the colon character and are case sensitive. The value of the parameter displays to the right of the colon character.
<pre>--config "parameter"</pre>	Displays the defined parameter value. If a value is added at the end of the command, the parameter updates with the new setting. The double



Option	Purpose
<code>name"</code> <code>["parameter</code> <code>value"]</code>	quote characters are required, although single quotes may be used when special characters are required. Note: While CLI changes to some parameters do not require restarting Tenable Nessus Network Monitor for the change to take effect, you must restart Tenable Nessus Network Monitor after changing the location of the realtime log file.
<code>-d debug mode</code>	Runs Tenable Nessus Network Monitor in debug mode for troubleshooting purposes. This option causes the system to use more resources and should be enabled only when directed by a Tenable Support Technician.
<code>-f packet_</code> <code>dump_file</code>	Replaces <code>packet_dump_file</code> with the path to the .pcap or .pcapng file you want Tenable Nessus Network Monitor to process. Note: Windows does not support the <code>pcapng</code> format.
<code>-h</code>	Displays the command line options help file.
<code>-k</code>	Displays the Tenable Nessus Network Monitor activation status.
<code>-L</code>	Displays a list of the license declarations.
<code>-l</code>	Displays a list of the plugin IDs that are loaded by Tenable Nessus Network Monitor.
<code>--list-</code> <code>interfaces</code>	Displays the interfaces that Tenable Nessus Network Monitor can access for packet collection. Useful to display interfaces to 10Gb cards running in high performance mode.
<code>-m</code>	Shows various aspects of memory usage during the processing of the <code>NNM</code> command.
<code>-p packet_</code> <code>dump_file</code>	Dumps payload packet data in Hex and ASCII to the specified <code>packet_dump_file</code> . This command dumps internal data from packet and plugins processing. This can be useful for debugging plugin issues.



Option	Purpose
<code>Tenable Nessus Network Monitor --users -add</code>	<p>Adds a new user to Tenable Nessus Network Monitor with the expected values of: ["username" "password" admin]: add new user. Expected values for "admin" flag are either: 1 - grant user administrative privileges, or 0 - don't grant user administrative privileges.</p> <p>Adds a new user to Tenable Nessus Network Monitor. Optionally, you can add the following arguments:</p> <p>NNM --users --add ["username" "password" admin]</p> <p>Expected values for "admin" flag are:</p> <ul style="list-style-type: none">• 1 - grant user administrative privileges• 0 - don't grant user administrative privileges
<code>Tenable Nessus Network Monitor --users -chpasswd</code>	<p>Changes an Tenable Nessus Network Monitor user's password.</p>
<code>Tenable Nessus Network Monitor --users -delete "user"</code>	<p>Removes a user from Tenable Nessus Network Monitor, where "user" is the username to be deleted.</p>
<code>--register-offline <license file></code>	<p>Registers Tenable Nessus Network Monitor in offline mode when you insert the license file obtained from Tenable®.</p>
<code>--config 'Software Update Type' <0-3></code>	<p>Configures the type of software update that runs when Tenable Nessus Network Monitor updates.</p> <ul style="list-style-type: none">0 - Disables all updates.1 - Updates only plugins.2 - Updates web server, HTML client, and plugins.3 - Updates all components (web server, HTML client, plugins, and



Option	Purpose
	engine).
--update-software <update package tarball>	Runs a software update using the setting you configured for Software Update Type. Optionally, if you are running Tenable Nessus Network Monitor in offline mode and have a custom update package, append the update package tarball name.
-v	Shows the version information about the installed instance of Tenable Nessus Network Monitor.



Linux Command Line Operations

You must run all commands with root privileges.

Start, Stop, or Restart Tenable Nessus Network Monitor

Action	Command to Manage Tenable Nessus Network Monitor
Start	<pre># service nnm start then # ps aux grep nnm</pre>
Stop	<pre># service nnm stop</pre>
Restart	<pre># service nnm restart</pre>

Once a day, as scheduled, if Tenable Security Center has received new Tenable Nessus Network Monitor plugins from Tenable®, it installs them in the Tenable Nessus Network Monitor plugin directory. Tenable Nessus Network Monitor detects the change, automatically reloads, and begins using the new plugins.

Real-time Tenable Nessus Network Monitor data is communicated to the configured Tenable Log Correlation Engine server or Syslog server(s) in real-time.

Configure HugePages

Before You Begin

These steps assume that your system meets the [System Requirements](#) necessary for running Tenable Nessus Network Monitor in High Performance mode.

To configure HugePages:

1. Ensure your HugePages settings are correct by using the following command:

```
# grep Huge /proc/meminfo  
AnonHugePages: 0kB
```



```
HugePages_Total: 1024
HugePages_Free: 1024
HugePages_Rsvd: 0
HugePages_Surp: 0
Hugepagesize: 2048kB
```

The **Hugepagesize** parameter is set to 2048 kB by default, but this option is configurable. Tenable Nessus Network Monitor requires a minimum of 1024 HugePages that are at least 2048 kB in size.

Note: In some cases, the `HugePages_Free` parameter may be set to 0, however, this does not necessarily indicate insufficient HugePage memory.

2. Reserve a certain amount of memory to be used as HugePages by using the following command to update the kernel parameter manually:

```
/bin/echo 1024 > /sys/devices/system/node/node0/hugepages/hugepages-2048kB/nr_hugepages
```

The number of HugePages reserved by the kernel changes to 1024, and HugePages become available.

Note: If the kernel does not have enough memory available to satisfy this request, the command may fail without notifying the user. After running this command, the HugePages configuration should be checked again using the command in step 1.

3. To ensure that your HugePages configuration persists across system reboots, refer to the following section that corresponds to your Linux kernel version.

CentOS 6

Update the persistent kernel configuration files using one of the following commands:

In the `/etc/sysctl.conf` file, add the `vm.nr_hugepages=1024` parameter and reload the kernel configuration with the `sysctl -p` command. Alternatively, you can reboot the system.

-or-



In the `/etc/grub.conf` file, on the kernel startup line, add the `hugepages=1024` parameter and reboot the system.

CentOS 7, 8

Update the persistent kernel configuration files using one of the following commands:

In the `/etc/sysctl.conf` file, add the `vm.nr_hugepages=1024` parameter and reload the kernel configuration with the `sysctl -p` command. Alternatively, you can reboot the system.

-or-

In the `/etc/sysconfig/grub` file, on the kernel startup command (`GRUB_CMDLINE_LINUX`), add the `hugepages=1024` parameter. Reload the kernel configuration with the `grub2-mkconfig -o /etc/grub2` command and reboot the system.

4. Connect the file system to the HugePages subsystem using the following steps:

- a. Execute the `/bin/mkdir -p /mnt/nnm_huge` command.
- b. Execute the `/bin/mount -t hugetlbfs nodev /mnt/nnm_huge` command.
- c. Additionally, open the `/etc/fstab` file location and add the following record:

```
nodev /mnt/nnm_huge hugetlbfs rw 0 0
```

File Locations

Tenable Nessus Network Monitor installs its files in the following locations:

Path	Purpose
<code>/opt/nnm</code>	Base directory.
<code>/opt/nnm/bin</code>	Location of the NNM and Tenable Nessus Network Monitor Proxy executables, plus several helper tools for the Tenable Nessus Network Monitor Proxy daemon.
<code>/opt/nnm/docs</code>	Contains the software license agreement for Tenable Nessus Network Monitor.
<code>/opt/nnm/var</code>	Contains the folders for Tenable Nessus Network Monitor and the Tenable Nessus Network Monitor-Proxy.



Path	Purpose
<code>/opt/nnm/var/nnm</code>	Contains plugins, discovered vulnerabilities, log files, keys, and other miscellaneous items.
<code>db</code>	Contains the database files related to the configuration, reports, and users for Tenable Nessus Network Monitor.
<code>kb</code>	Stores the Tenable Nessus Network Monitor knowledge base, if used.
<code>logs</code>	Contains Tenable Nessus Network Monitor logs.
<code>plugins</code>	Contains the Tenable Nessus Network Monitor plugins delivered via Tenable Security Center, Tenable Vulnerability Management, the Tenable Nessus Network Monitor Feed, or updated via the command line or web interface if Tenable Nessus Network Monitor is running in Offline mode. <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;">Note: If Tenable Security Center is used to manage the plugins, do not change this path from the default <code>/opt/nnm/var/nnm</code>.</div>
<code>nnm-services</code>	A file Tenable Nessus Network Monitor uses to map service names to ports. This file may be edited by the user. Plugin updates do not overwrite modifications to the file.
<code>reports</code>	Contains reports generated by Tenable Nessus Network Monitor. This folder contains the <code>.nessus</code> file generated by default.
<code>scripts</code>	Contains the files for the Tenable Nessus Network Monitor Web server.
<code>ssl</code>	Contains SSL certificates used by the proxy and web server for the SSL connection between itself and Tenable Security Center or the web browser.
<code>users</code>	Contains folders for user files and reports.
<code>www</code>	Contains the files for the Tenable Nessus Network Monitor web front-end.



Path	Purpose
/opt/nnm/var/nnm-proxy	Parent folder for files used/created by the Tenable Nessus Network Monitor proxy.
logs	Contains the Tenable Nessus Network Monitor proxy and Tenable Nessus Network Monitor proxy service logs.



Windows Command Line Operations

You must run all programs as a local user with administrative privileges. To do so, when UAC is enabled, right-click on the installer program and select **Run as Administrator**.

Start or Stop Tenable Nessus Network Monitor

Action	Command to Manage Tenable Nessus Network Monitor
Start	<code>net start "Tenable Tenable Nessus Network Monitor Proxy"</code>
Stop	<code>net stop "Tenable Tenable Nessus Network Monitor Proxy"</code>

Alternatively, Tenable Nessus Network Monitor can be managed via the **Services** control panel utility. Under the list of services, find **Tenable Tenable Nessus Network Monitor Proxy Service**. Right click on the service to provide a list of options for the services, including the ability to start or stop the **Tenable Tenable Nessus Network Monitor** or **Tenable Tenable Nessus Network Monitor Proxy** service.

File Locations

Tenable Nessus Network Monitor installs its files in the following locations:

Path	Purpose
C:\Program Files\Tenable\NNM	Contains Tenable Nessus Network Monitor binaries and dependent libraries.
C:\ProgramData\Tenable\NNM	Contains all data files consumed and output by Tenable Nessus Network Monitor and Tenable Nessus Network Monitor Proxy (e.g., configuration, plugins, logs, and reports).

Note: This directory does not appear unless the Windows Hidden Files and Folders option is enabled.

The following table contains the folder layout under **C:\ProgramData\Tenable\NNM**:



Folder	Purpose
docs	Contains the software license agreement for Tenable Nessus Network Monitor.
NNM	Parent folder for Tenable Nessus Network Monitor logs, reports, plugins, and scripts directories. Also contains the Tenable Nessus Network Monitor-services file.
db	Contains the database files relating to the configuration, reports, and users for Tenable Nessus Network Monitor.
kb	Stores the Tenable Nessus Network Monitor knowledge base, if used.
logs	Contains Tenable Nessus Network Monitor logs.
plugins	Contains the Tenable Nessus Network Monitor plugins delivered via Tenable Security Center, Tenable Vulnerability Management, the Tenable Nessus Network Monitor Feed, or updated via the command line or web interface if Tenable Nessus Network Monitor is running in Offline mode. <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;">Note: Do not change this path from the default C:\ProgramData\Tenable\NNM\nnm if Tenable Security Center is used to manage the plugins.</div>
nmm-services	A file Tenable Nessus Network Monitor uses to map service names to ports. This file may be edited by the user. Plugin updates do not overwrite modifications to the file.
reports	Contains reports generated by Tenable Nessus Network Monitor . This folder contains the .nessus file generated by default.
scripts	Contains the files for the Tenable Nessus Network Monitor Web server.
ssl	Contains SSL certificates used by the proxy and web server for the SSL connection between itself and Tenable Security Center or the web browser.
users	Contains folders for user files and reports.
www	Contains the files for the Tenable Nessus Network Monitor web front-end.



Folder	Purpose
nnm-proxy	Parent folder for files used/created by the Tenable Nessus Network Monitor proxy.
logs	Contains Tenable Nessus Network Monitor proxy and Tenable Nessus Network Monitor proxy service logs.
run	Contains process ID temporary files.



macOS Command Line Operations

You must run all programs as a root user or with equivalent privileges.

Start or Stop Tenable Nessus Network Monitor

Action	Command to Manage Tenable Nessus Network Monitor
Start	<code># launchctl load -w /Library/LaunchDaemons/com.tenablesecurity.nnm-proxy.plist</code>
Stop	<code># launchctl unload -w /Library/LaunchDaemons/com.tenablesecurity.nnm-proxy.plist</code>

File Locations

Tenable Nessus Network Monitor installs its files in the following locations:

Path	Purpose
<code>/Library/NNM</code>	Base directory.
<code>/Library/NNM/docs</code>	Contains the Tenable Nessus Network Monitor license agreement in various file formats.
<code>/Library/NNM/bin</code>	Location of the NNM and Tenable Nessus Network Monitor Proxy executables, plus several helper tools for the Tenable Nessus Network Monitor Proxy daemon.
<code>/Library/NNM/var/nnm</code>	Contains plugins, discovered vulnerabilities, log files, keys, and other miscellaneous items.
<code>db</code>	Contains the database files related to the configuration, reports, and users for Tenable Nessus Network Monitor.
<code>kb</code>	Stores the Tenable Nessus Network Monitor knowledge base, if used.
<code>logs</code>	Contains Tenable Nessus Network Monitor logs.



Path	Purpose
plugins	<p>Contains the Tenable Nessus Network Monitor plugins delivered via Tenable Security Center, Tenable Vulnerability Management, the Tenable Nessus Network Monitor Feed, or updated via the command line or web interface if Tenable Nessus Network Monitor is running in Offline mode.</p> <div style="border: 1px solid blue; padding: 5px;"><p>Note: Do not change this path from the default <code>/Library/NNM/var/nnm</code> if Tenable Security Center is used to manage the plugins.</p></div>
nnm-services	<p>A file Tenable Nessus Network Monitor uses to map service names to ports. This file may be edited by the user. Plugin updates do not overwrite modifications to the file.</p>
reports	<p>Contains reports generated by Tenable Nessus Network Monitor. This folder contains the <code>.nessus</code> file generated by default.</p>
scripts	<p>Contains the files for the Tenable Nessus Network Monitor Web server.</p>
ssl	<p>Contains SSL certificates used by the proxy and web server for the SSL connection between itself and Tenable Security Center or the web browser.</p>
users	<p>Contains files and reports for Tenable Nessus Network Monitor users.</p>
www	<p>Contains the files for the Tenable Nessus Network Monitor web front-end.</p>
/Library/NNM/var/nnm-proxy	<p>Parent folder for files used/created by the Tenable Nessus Network Monitor proxy.</p>
logs	<p>Contains the Tenable Nessus Network Monitor proxy and Tenable Nessus Network Monitor proxy service logs.</p>



Configure Tenable Nessus Network Monitor for Certificates

To allow SSL certificate authentication, you must first configure the Tenable Nessus Network Monitor web server with a server certificate and CA.

This process allows the web server to trust certificates created by the CA for authentication purposes. Generated files related to certificates must be owned by root:root and, by default, have the correct permissions.

This section contains the following instructions:

- [Create a Custom CA and Server Certificate](#)
- [Create Tenable Nessus Network Monitor SSL Certificates for Login](#)
- [Connect to Tenable Nessus Network Monitor with a User Certificate](#)



Create a Custom CA and Server Certificate

To create a custom CA and server certificate:

1. Optionally, create a new custom CA and server certificate for the Tenable Nessus Network Monitor server using the `NNM-make-cert` command. This places the certificates in the correct directories.
2. When prompted for the host name, type the DNS name or IP address of the server in the browser (eg., `https://hostname:8835/` or `https://ipaddress:8835/`). The default certificate uses the host name.
3. If you wish to use a CA certificate instead of the Tenable Nessus Network Monitor generated one, make a copy of the self-signed CA certificate using the appropriate command for your OS:

Operating System	Command
Linux	<pre># cp /opt/nnm/var/nnm/ssl/cacert.pem /opt/nnm/var/nnm/ssl/ORIGcacert.pem</pre>
Windows	<pre>copy \ProgramData\Tenable\NNM\nnm\ssl\cacert.pem C:\ProgramData\Tenable\NNM\nnm\ssl\ORIGcacert.pem</pre>
macOS	<pre># cp /Library/NNM/var/nnm/ssl/cacert.pem /Library/NNM/var/nnm/ssl/ORIGcacert.pem</pre>

4. If the authentication certificates are created by a CA other than the Tenable Nessus Network Monitor server, the CA certificate must be installed on the Tenable Nessus Network Monitor server. Copy the organization's CA certificate to the appropriate location for your OS:

Operating System	File Location
Linux	<code>/opt/nnm/var/nnm/ssl/cacert.pem</code>
Windows	<code>C:\ProgramData\Tenable\NNM\nnm\ssl\cacert.pem</code>
macOS	<code>/Library/NNM/var/nnm/ssl/cacert.pem</code>



5. Once the CA is in place, restart the Tenable Nessus Network Monitor services.
6. After Tenable Nessus Network Monitor is configured with the proper CA certificate(s), users may log in to Tenable Nessus Network Monitor using SSL client certificates.



Create Tenable Nessus Network Monitor SSL Certificates for Login

You can log in to an Tenable Nessus Network Monitor server with SSL certificates. Once certificate authentication is enabled, username and password login is disabled. You must create the certificates using the `nnm-make-cert` command.

Note: When asked if you want to create a server certificate, select **no** to be prompted for the user certificate information.

To create Tenable Nessus Network Monitor SSL certificates for login:

1. On the Tenable Nessus Network Monitor server, run the `nnm-make-cert` command.

Operating System	Command
Linux	<code># /opt/nnm/bin/nnm-make-cert</code>
Windows	<code>C:\Program Files\Tenable\NNM\nnm-make-cert</code>
macOS	<code># /Library/NNM/bin/nnm-make-cert</code>

2. Configure the client certificate by answering the various questions.

Two files, the certificate and the key, are created in the temporary directory.

Operating System	Directory
Linux	<code>/opt/nnm/var/nnm/temp</code>
Windows	<code>C:\ProgramData\Tenable\NNM\nnm\temp</code>
macOS	<code>/Library/NNM/nnm/var/temp</code>

3. Combine and export the certificate and key file into a format that can be imported into the web browser, such as `.pfx`.

In the following example where the username is `admin`, the files `cert_admin.pem` and `key_admin.pem` are combined into the file `combined_admin.pfx`.



Note: The username you type must correspond with an existing username in Tenable Nessus Network Monitor. By default, Tenable Nessus Network Monitor has only one administrative user. If you add another administrative user, then you can use more than one certificate.

```
openssl pkcs12 -export -out combined_admin.pfx -inkey key_admin.pem -in cert_admin.pem -chain -CAfile /opt/nnm/var/nnm/ssl/cacert.pem -passout 'pass:password' -name 'Tenable Nessus Network Monitor User Certificate for: admin'
```

The resulting file is created in the directory from which the command was launched.

Note: If your Tenable Nessus Network Monitor is managed by Tenable Security Center you must concatenate the *cert_admin.pem* and *key_admin.pem* files into a new file (for example, "*sc_admin.pem*"). Upload this file to Tenable Security Center to log on to NNM using SSL certificates.

4. Import the combined file into the web browser's personal certificate store.
5. Configure the Tenable Nessus Network Monitor server for certificate authentication using the appropriate command for your operating system.

Once certificate authentication is enabled, username and password login is disabled.

Operating System	Command
Linux	<code># /opt/nnm/bin/nnm --config "Enable SSL Client Certificate Authentication" "1"</code>
Windows	<code>C:\Program Files\Tenable\NNM\nnm --config "Enable SSL Client Certificate Authentication" "1"</code>
macOS	<code># /Library/NNM/bin/nnm --config "Enable SSL Client Certificate Authentication" "1"</code>



Connect to Tenable Nessus Network Monitor with a User Certificate

To connect to Tenable Nessus Network Monitor with a user certificate:

1. In a web browser, navigate to `https://<ip address or hostname>:8835`.

The browser displays a list of available certificates.

2. Select the appropriate certificate.

The certificate becomes available for the current Tenable Nessus Network Monitor session.

3. Click the **Sign In** button.

You are automatically logged in as the designated user and Tenable Nessus Network Monitor can be used normally.

Note: If you log out of Tenable Nessus Network Monitor, the standard Tenable Nessus Network Monitor login screen appears. If you want to log in with the same certificate, refresh your browser. If you want to use a different certificate, restart your browser session.



Custom SSL Certificates

By default, Tenable Nessus Network Monitor is installed and managed using HTTPS and SSL support and uses port 8835. Default installations of Tenable Nessus Network Monitor use a self-signed SSL certificate.

To avoid browser warnings, use a custom SSL certificate specific to your organization. During the installation, Tenable Nessus Network Monitor creates two files that make up the certificate: `servercert.pem` and `serverkey.pem`. Replace these files with certificate files generated by your organization or a trusted CA. Also, you may have to update `cacert.pem` and `cakey.pem` if your `servercert.pem` is signed by intermediate CAs.

A certificate chain link from your `servercert.pem` certificate must be defined where the subject/issuer pairs of intermediate CAs match all the way to a root certificate or there is a link to the signing CA in the final intermediate CA. The certificate chain can be defined in `cacert.pem` or a `serverchain.pem` file. Use the `openssl s_client` utility to troubleshoot your certificate chains. You may have to consult with a PKI expert to set up your certificates. For example, `openssl s_client -connect host_name:8835 -state -debug` shows the certificates being used and the subject/issuer chain link.

Before replacing the certificate files:

1. Stop the Tenable Nessus Network Monitor server.
2. Back up the original files in case you need to restore them.
3. Replace the files and re-start the Tenable Nessus Network Monitor server.

Note: If the certificate is generated by a trusted CA, subsequent connections to the scanner do not show an error.

Certificate File Locations

Operating System	Directory
Linux	<code>/opt/nnm/var/nnm/ssl/servercert.pem</code> <code>/opt/nnm/var/nnm/ssl/serverkey.pem</code>
Windows	<code>C:\ProgramData\Tenable\NNM\nnm\ssl\servercert.pem</code> <code>C:\ProgramData\Tenable\NNM\nnm\ssl\serverkey.pem</code>



Operating System	Directory
macOS	<code>/Library/NNM/var/nnm/ssl/servercert.pem</code> <code>/Library/NNM/var/nnm/ssl/serverkey.pem</code>

Optionally, you can use the `/getcert` switch to install the root CA in your browser, which removes the warning:

`https://<IP address>:8835/getcert`

To set up an intermediate certificate chain, place a file named `serverchain.pem` in the same directory as the `servercert.pem` file.

This file must contain the 1-n intermediate certificates (concatenated public certificates) necessary to construct the full certificate chain from the Tenable Nessus Network Monitor server to its ultimate root certificate (one trusted by the user's browser).

SSL Client Certificate Authentication

Tenable Nessus Network Monitor supports use of SSL client certificate authentication. When the browser is configured for this method, the use of SSL client certificates is allowed.

Tenable Nessus Network Monitor allows for password-based or SSL Certificate authentication methods for user accounts. When creating a user for SSL certificate authentication, use the Tenable Nessus Network Monitor-make-cert-client utility through the command line on the Tenable Nessus Network Monitor server.



Configure Tenable Nessus Network Monitor for NIAP Compliance

If your organization requires that your instance of Tenable Nessus Network Monitor meets National Information Assurance Partnership (NIAP) standards, you can configure Tenable Nessus Network Monitor so that relevant settings are compliant with NIAP standards.

Before you begin:

- Ensure you are running Tenable Nessus Network Monitor version 5.12.06.2.0 or later.
- If you are using SSL certificates to log in to Tenable Nessus Network Monitor, ensure your server and client certificates are NIAP compliant.
- To force all passwords to use NIAP-compliant hashing, the administrator must force resets on all passwords.
- Confirm you have enabled the full disk encryption capabilities provided by the operating system on the host where Tenable Nessus Network Monitor is installed.

Tenable Nessus Network Monitor 6.1.x supports OpenSSL 3.0.0 and later. Tenable Nessus Network Monitor 6.2.1 supports OpenSSL 3.0.8. Open SSL 3.0.x exhibits the following behaviors and limitations:

- OpenSSL 3.0.x is more strict with SSL Client Certificates than OpenSSL 1.1.1.
- SSL certificates that do not include the **Authority Key Identification** or **Subject Key Identification** sections are not valid in OpenSSL 3.0.7 and later.
- NIAP Mode in Tenable Nessus Network Monitor will not allow connections if the user's SSL client certificate does not have the required sections.
- If your SSL certificate includes OCSP servers in the **Authority Information Access** section, these OCSP servers will be used to verify your certificate. Those servers must have **OCSP Signing** enabled in the **Extended Key Usage** section.
- The Tenable Nessus Network Monitor User Interface does not allow the user to enable the NIAP option unless the SSL certificate provides the required sections.

To configure Tenable Nessus Network Monitor for NIAP compliance:



1. Log in to Tenable Nessus Network Monitor using one of the following methods:
 - Username and password.
 - SSL certificates, as described in [Connect to Tenable Nessus Network Monitor with a User Certificate](#).
2. Set the Tenable Nessus Network Monitor web server to use TLS 1.2 communications:

- a. Click the  button.

- b. Click **Configuration**.

By default, the **NNM Settings** section appears.

- c. In the **Setting Type** drop-down menu, select **NNM Web Server**.

- d. Set **Use TLS 1.2** to **Enabled**.

3. Enable NIAP mode:

- In the user interface:

- a. Click the  button.

- b. Click **Configuration**.

By default, the **NNM Settings** section appears.

- c. In the **Setting Type** drop-down menu, select **AdvancedSecurity Options**.

- d. Set **Enable FIPS Mode**.

- e. Set **Enable NIAP Mode** to 1.

- In the command line interface:

- a. Access Tenable Nessus Network Monitor from a command line interface.

- b. In the command line, enter the following command:

```
nmn --config "Enable FIPS Mode" 1
```



Linux example:

```
/opt/nnm/bin/nnm --config "Enable FIPS Mode" 1
```

c. In the command line, enter the following command:

```
nnm --config "Enable NIAP Mode" 1
```

Linux example:

```
/opt/nnm/bin/nnm --config "Enable NIAP Mode" 1
```

- Tenable Nessus Network Monitor does the following:
 - Verifies that Tenable Nessus Network Monitor is using TLS 1.2.
 - Regardless of the **Enable Strong Encryption** setting, Tenable Nessus Network Monitor overrides the selected cipher suites with the following ciphers: ECDHE-RSA-AES128-SHA256 : ECDHE-RSA-AES128-GCM-SHA256 : ECDHE-RSA-AES256-SHA384 : ECDHE-RSA-AES256-GCM-SHA384

Note: When Tenable Nessus Network Monitor is in NIAP mode, Tenable Nessus Network Monitor overrides the cipher suites as long as Tenable Nessus Network Monitor remains in NIAP mode. If you disable NIAP mode, Tenable Nessus Network Monitor reverts to what you had set before.

- Tenable Nessus Network Monitor uses strict certificate validation:
 - Disallows certificate chains if any intermediate certificate lacks the CA extension.
 - Authenticates a server certificate, using the signing CA certificate.
 - Authenticates a client certificate when using client certificate authentication for login.
 - OCSP servers with certificates that do not have **OCSP Signing** in the **Extended Key Usage** section are disallowed and the connection will be



terminated, per the requirements specified by NIAP standards.

- Checks the revocation status of a CA certificate using the Online Certificate Status Protocol (OCSP). If the response is that the certificate is revoked or has an unknown CA, then the certificate will be marked as invalid. If the OCSP server is down and there is no response, then the certificate will not be marked as invalid, and its use will be permitted if it is otherwise valid.

Database Encryption

You can convert encrypted databases from the default format (OFB-AES-128) to NIAP-compliant encryption (XTS-AES-256).

Tenable Nessus Network Monitor in NIAP mode can read databases with the default format (OFB-AES-128).

To convert encrypted databases to NIAP-compliant encryption:

1. [Stop Tenable Nessus Network Monitor](#).
2. Ensure NIAP mode is enabled, as described in the previous procedure.
3. [Stop Tenable Nessus Network Monitor](#).
4. Monitor the files in `/opt/nnm/var/nnm/db` to ensure there are no `.db_shm` or `.db_wal` temporary files in the directory.
5. Enter the following command:

```
nm security niapconvert
```

Tenable Nessus Network Monitor converts encrypted databases to XTS-AES-256 format.



Encryption Strength

Tenable Nessus Network Monitor uses the following default encryption for storage and communications.

Note: If your organization requires that your instance of Tenable Nessus Network Monitor meets National Information Assurance Partnership (NIAP) standards, certain settings may be configured differently than the following information. For more information, see [Configure Tenable Nessus Network Monitor for NIAP Compliance](#)

Function	Encryption
Storing user account passwords	SHA-512 and the PBKDF2 function with a 512 bit key
Database encryption	OFB-AES-128 XTS-AES-256 when configured for NIAP compliance .
Passphrase for SSL browser certificates	Tenable Nessus Network Monitor does not store passphrases for any certificates. For information on how OpenSSL encrypts and stores passphrases for SSL certificates, see the OpenSSL documentation.
Communications between Tenable Nessus Network Monitor and clients (Tenable Nessus Network Monitor user interface users).	TLS 1.2 with the strongest encryption method supported by Tenable Nessus Network Monitor and your browser. For information on cipher suites used, see Enable Strong Encryption . Cipher suites are overridden when configured for NIAP compliance .
Communications between Tenable Nessus Network Monitor and the Tenable product registration server	TLS 1.2 with ECDHE-RSA-AES256-GCM-SHA384.



Communications between Tenable Nessus Network Monitor and the Tenable plugin update server

TLS 1.2 with ECDHE-RSA-AES256-GCM-SHA384.



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, you should add Tenable Nessus Network Monitor to the allow list.

The following table contains a list of Tenable Nessus Network Monitor folders, files, and processes that should be allowed.

Note: If your Windows installation uses a non-standard drive or folder structure, use the %PROGRAMFILES% and %PROGRAMDATA% environment variables.

Windows
Files
C:\Program Files\Tenable\NNM*
C:\ProgramData\Tenable\NNM*
Processes
C:\Program Files\Tenable\NNM\nnm.exe
C:\Program Files\Tenable\NNM\nnm-proxy.exe
C:\Program Files\Tenable\NNM\nnm-proxy-service.exe
Linux
Files (for RHEL 6/CentOS 6 and compatible distributions)
/opt/nnm/*
/etc/init.d/nnm
Files (for RHEL 7/CentOS 7 and later, and compatible distributions like Oracle Linux)
/opt/nnm/*
/usr/lib/systemd/system/nnm.service
/usr/lib/systemd/system/nnm-proxy.service
Processes



/opt/nnm/bin/nnm

/opt/nnm/bin/nnm-proxy

macOS

Files

/Library/NNM/*

Processes

/Library/NNM/bin/nnm

/Library/NNM/bin/nnm-proxy



Modules

Tenable Nessus Network Monitor includes analysis modules that analyze network traffic based on certain criteria. These modules modularize Tenable Nessus Network Monitor detection capabilities and provide users the ability to enable or disable them. There are two analysis modules:

- **SCADA/ICS Analysis Module**

- **Note:** This module is only available for Industrial Security customers.

Industrial Security is end-of-life (EOL). For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle [Matrix](#) and [Policy](#).

This module analyzes SCADA network traffic to discover SCADA assets and their vulnerabilities. In addition, the module provides deep visibility into the type of SCADA devices discovered. This module is enabled by default and can be disabled in environments that do not contain SCADA devices. You can use the [Tenable Search](#) page to search for specific device detection information. This module is only available for Industrial Security customers.

- **Connection Analysis Module**

This module reports connection duration and bandwidth information including for IPv6 and tunneled traffic. This module is disabled by default.

Note: You must restart Tenable Nessus Network Monitor after enabling a module for the module to function correctly within Tenable Nessus Network Monitor.

Connection Analysis Module

Module Detection ID	Module Detection Name	Module Detection Description	Risk Factor
97	TCP Session Bandwidth (1 - 10 MB)	Tenable Nessus Network Monitor computes the bytes exchanged between each TCP endpoint when the session ends. The total bytes exchanged during the lifetime of this session is between 1 and 10 MB.	INFO
98	TCP Session Bandwidth (10 - 100 MB)	Tenable Nessus Network Monitor computes the bytes exchanged between each TCP endpoint when the session ends. The total bytes exchanged during the lifetime of this session is more than 10 MB but less than or equal to 100 MB.	INFO
99	TCP Session Bandwidth (100 MB - 1 GB)	Tenable Nessus Network Monitor computes the bytes exchanged between each TCP endpoint when the session ends. The total bytes exchanged during the lifetime of this session is more than 100 MB but less than or equal to 1 GB.	INFO
100	TCP Session Bandwidth (> 1 GB)	Tenable Nessus Network Monitor computes the bytes exchanged between each TCP endpoint when the session ends. The total bytes exchanged during the lifetime of this session is more than 1 GB.	INFO



Module Detection ID	Module Detection Name	Module Detection Description	Risk Factor
	GB)	Monitor computes the bytes exchanged between each TCP endpoint when the session ends. The total bytes exchanged during the lifetime of this session is more than 1 GB.	
101	TCP Session Duration (< 1 minute)	Tenable Nessus Network Monitor computes the duration of each TCP session when the session ends. This TCP session duration is less than 1 minute.	INFO
102	TCP Session Duration (1 - 15 minutes)	Tenable Nessus Network Monitor computes the duration of each TCP session when the session ends. This TCP session duration is between 1 minute and 15 minutes.	INFO
103	TCP Session Duration (15 - 25 minutes)	Tenable Nessus Network Monitor computes the duration of each TCP session when the session ends. This TCP session duration is more than 15 but less than or equal to 25 minutes.	INFO
104	TCP Session Duration (25 - 40	Tenable Nessus Network	INFO



Module Detection ID	Module Detection Name	Module Detection Description	Risk Factor
	minutes)	Monitor computes the duration of each TCP session when the session ends. This TCP session duration is more than 25 but less than or equal to 40 minutes.	
105	TCP Session Duration (40 - 55 minutes)	Tenable Nessus Network Monitor computes the duration of each TCP session when the session ends. This TCP session duration is more than 40 but less than or equal to 55 minutes.	INFO
106	TCP Session Duration (55 - 100 minutes)	Tenable Nessus Network Monitor computes the duration of each TCP session when the session ends. This TCP session duration is more than 55 but less than or equal to 100 minutes.	INFO
107	TCP Session Duration (100 minutes - 24 hours)	Tenable Nessus Network Monitor computes the duration of each TCP session when the session ends. This TCP session duration is more than 100 minutes but less than or equal to 24	INFO



Module Detection ID	Module Detection Name	Module Detection Description	Risk Factor
		hours.	
108	TCP Session Duration (24 - 47 hours)	Tenable Nessus Network Monitor computes the duration of each TCP session when the session ends. This TCP session duration is more than 24 hours but less than or equal to 47 hours.	INFO
109	TCP Session Duration (> 47 hours)	Tenable Nessus Network Monitor computes the duration of each TCP session when the session ends. This TCP session duration is more than 47 hours.	INFO
110	UDP Activity	UDP activity observed	INFO
111	ICMP Activity	ICMP activity observed	INFO
112	IGMP Activity	IGMP activity observed	INFO



Tenable Nessus Network Monitor Plugins

This section provides the following information about Tenable Nessus Network Monitor plugins:

- [Vulnerability and Passive Fingerprinting](#)
- [Tenable Nessus Network Monitor Fingerprinting](#)
- [Tenable Nessus Network Monitor Plugin Syntax](#)
- [Tenable Nessus Network Monitor Real-Time Plugin Syntax](#) and [Examples](#)
- [Tenable Nessus Network Monitor Corporate Policy Plugins](#)



About Tenable Nessus Network Monitor Plugins

Tenable Nessus Network Monitor has two sources of plugin information: the `.prmx` and `.prm` plugin libraries in the `plugins` directory.

Tenable distributes its passive vulnerability plugin database in an encrypted format. The encrypted file is named `tenable_plugins.prmx` and, if necessary, can be updated daily. Tenable Nessus Network Monitor plugins written by the customer or third parties have the `.prm` extension.

Tenable has also implemented passive fingerprinting technology based on the open-source **SinFP** tool. With permission from the author, Tenable includes the database of passive operating system fingerprints for the fingerprinting technology in this distribution of Tenable Nessus Network Monitor.

Writing Custom Plugins

Tenable Nessus Network Monitor customers can write their own passive plugins, which are added into the `plugins` directory in the Tenable Nessus Network Monitor installation directory. The plugin must end with a `.prm` extension to be visible by Tenable Nessus Network Monitor.

You must restart Tenable Nessus Network Monitor if:

- You add a new custom plugin to the `plugins` directory. Tenable Nessus Network Monitor does not fire the plugin until you restart.
- You delete a `.prm` file manually from the `plugins` directory. Tenable Nessus Network Monitor continues to fire the plugin until you restart.



Tenable Nessus Network Monitor Fingerprinting

Tenable uses a hybrid approach to operating system fingerprinting. Primarily, plugins are used to detect and identify the OS of a host. If this is not possible, Tenable Nessus Network Monitor uses detected packets to identify the OS.

Tenable Nessus Network Monitor has the ability to guess the operating system of a host by looking at the packets it generates. Specific combinations of TCP packet entries, such as the window size and initial time-to-live (TTL) values, allow Tenable Nessus Network Monitor to predict the operating system generating the traffic.

These unique TCP values are present when a server makes or responds to a TCP request. All TCP traffic is initiated with a “SYN” packet. If the server accepts the connection, it sends a response known as a “SYN-ACK” packet. If the server cannot or will not communicate, it sends a reset (RST) packet. When a server sends a “SYN” packet, Tenable Nessus Network Monitor applies these list of operating system fingerprints and attempts to determine the operating system type.

Tenable Network Security has permission to re-distribute the passive operating fingerprints from the author of [SinFP open source project](#).



Tenable Nessus Network Monitor Plugin Syntax

Plugins

Tenable Nessus Network Monitor plugins allow spaces and comment fields that start with a number (#) sign. Each plugin must be separated with the word “NEXT” on a single line. Create a `.prm` file in the `plugins` directory to make it available for use. You must restart Tenable Nessus Network Monitor to use new custom plugins.

Plugin Keywords

There are several keywords available for writing passive vulnerability plugins for Tenable Nessus Network Monitor. Some of these keywords are mandatory and some are optional. In the table below, mandatory keywords are boldened.

Name	Description
<code>bid</code>	Tenable assigns SecurityFocus Bugtraq IDs (BID) to Tenable Nessus Network Monitor plugins. This allows a user reading a report generated by Tenable Nessus Network Monitor to link to more information available at http://www.securityfocus.com/bid . Multiple Bugtraq entries can be typed on one line if separated by commas.
<code>bmatch</code>	This is the same as <code>match</code> but can look for any type of data. A <code>bmatch</code> must always have an even number of alphanumeric characters.
<code>clientissue</code>	If a vulnerability is determined in a network client such as a web browser or an email tool, a server <code>port</code> is associated with the reported vulnerability.
<code>cve</code>	Tenable also assigns Common Vulnerability and Exposure (CVE) tags to each Tenable Nessus Network Monitor plugin. This allows a user reading a report generated by Tenable Nessus Network Monitor to link to more information available at http://cve.mitre.org/ . Multiple CVE entries can be typed on one line if separated by commas.



Name	Description
<code>dependency</code>	This is the opposite of <code>noplugin</code> . Instead of specifying another plugin that has failed, this keyword specifies which plugin must succeed. This keyword specifies a Tenable Nessus Network Monitor ID that should exist to evaluate the plugin. In addition, this plugin can take the form of <code>dependency=ephemeral-server-port</code> , which means the evaluated server must have an open port above port 1024.
<code>dport</code>	This is the same as <code>sport</code> , but for destination ports.
<code>Exploitability:</code> <code>canvas</code> <code>core</code> <code>cvsstemporal</code> <code>metasploit</code>	Displays exploitability factors for the selected vulnerability. For example, if the vulnerability is exploitable via both Canvas and Core and has a unique CVSS temporal score, the following tags may be displayed in the plugin output: CANVAS : D2ExploitPack CORE : true CVSSTEMPORAL : CVSS2#E:F/RL:OF/RC:C
<code>family</code>	Each Tenable plugin for Tenable Nessus Network Monitor is included in a family. This designation allows Tenable to group Tenable Nessus Network Monitor plugins into easily managed sets that can be reported on individually.
<code>hs_dport</code>	This is the same as <code>hs_sport</code> except for destination ports.
<code>hs_sport</code>	Normally, when Tenable Nessus Network Monitor runs its plugins, they are either free ranging looking for matches on any port, or fixed to specific ports with the <code>sport</code> or <code>dport</code> keywords. In very high speed networks, many plugins have a fallback port, known as a high-speed port, which focuses the plugin only on one specific port. In High Performance mode, the performance of a Tenable Nessus Network Monitor plugin with an <code>hs_sport</code> keyword is exactly the same as if the plugin was written with the <code>sport</code> keyword.



Name	Description
<code>id</code>	Each Tenable Nessus Network Monitor plugin needs a unique rule ID. Tenable assigns these 16 bit numbers within the overall Tenable Nessus Network Monitor range of valid entries. A list of the current Tenable Nessus Network Monitor plugin IDs can be found on the Tenable website .
<code>match</code>	This keyword specifies a set of one or more simple ASCII patterns that must be present in order for the more complex pattern analysis to take place. The <code>match</code> keyword gives Tenable Nessus Network Monitor a lot of its performance and functionality. With this keyword, if it does not see a simple pattern, the entire plugin does not match.
<code>name</code>	This is the name of the vulnerability Tenable Nessus Network Monitor has detected. Though multiple Tenable Nessus Network Monitor plugins can have the same name, it is not encouraged.
<code>nid</code>	To track compatibility with the Tenable Nessus vulnerability scanner, Tenable associates Tenable Nessus Network Monitor vulnerability checks with relevant Tenable Nessus vulnerability checks. Multiple Tenable Nessus IDs can be listed under one <code>nid</code> entry such as <code>nid=10222,10223</code> .
<code>nooutput</code>	For plugins that are written specifically to be used as part of a dependency with another plugin, the <code>nooutput</code> keyword causes Tenable Nessus Network Monitor not to report anything for any plugin with this keyword enabled.
<code>noplugin</code>	This keyword prevents a plugin from being evaluated if another plugin has already matched. For example, it may make sense to write a plugin that looks for a specific anonymous FTP vulnerability, but disable it if another plugin that checked for anonymous FTP has already failed.
<code>pbmatch</code>	This is the same as <code>bmatch</code> except for binary data on the previous side of the reconstructed network session.



Name	Description
<code>plugin_output</code>	This keyword displays dynamic data for a given vulnerability or event. The dynamic data is usually represented using %L or %P, and its value is obtained from the regular expressions defined using <code>regex</code> , <code>regexi</code> , <code>pregex</code> , or <code>pregexi</code> .
<code>pmatch</code>	This keyword is the same as <code>match</code> but is applied against the previous packet on the other side of the reconstructed network session.
<code>pregex</code>	This is the same as <code>regex</code> except the regular expression is applied to the previous side of the reconstructed network session.
<code>pregexi</code>	This is the same as <code>pregex</code> except the pattern matching is not case sensitive.
<code>protocol_id</code>	This keyword is used to specify the protocol number of the protocol causing the plugin to fire.
<code>regex</code>	This keyword specifies a complex regular expression search rule applied to the network session.
<code>regexi</code>	This is the same as <code>regex</code> except the pattern matching is not case sensitive.
<code>risk</code>	All Tenable Nessus Network Monitor plugins need a risk setting. Risks are classified as INFO, LOW, MEDIUM, HIGH, and CRITICAL. An INFO risk is an informational vulnerability such as client or server detection. A LOW risk is an informational vulnerability such as an active port or service. A MEDIUM risk is something that may be exploitable or discloses information. A HIGH risk is something that is easily exploitable. A CRITICAL risk is something that is very easily exploitable and allows for malicious attacks.
<code>seealso</code>	If one or more URLs are available, this keyword can be used to display them. Multiple URLs can be specified on one line if separated by commas. Example entries for this include CERT advisories and



Name	Description
	vendor information websites.
<code>solution</code>	If a solution is available, it can be described here. The report section highlights the solution with different text.
<code>sport</code>	This setting applies the Tenable Nessus Network Monitor plugin to just one port. For example, you may wish to write a SNMP plugin that just looks for activity on port 162. However, for detection of off-port services like a web server running on port 8080, a <code>sport</code> field is not used in the plugin.
<code>stripped_description</code>	This field describes on one line the nature of the detected vulnerability. This data is printed out by Tenable Nessus Network Monitor when printing the vulnerability report. Macros are available that allow the printing of matched network traffic such as banner information and are discussed in the examples below. For line breaks, the characters “\n” can be used to invoke a new line.
<code>timed-dependency</code>	This keyword slightly modifies the functionality of the <code>noplugin</code> and <code>dependency</code> keywords such that the evaluation must have occurred within the last <i>N</i> seconds.
<code>udp</code>	This keyword specifies that plugins are to be based on the UDP protocol rather than TCP protocol.

Tip: In addition to `tcp` or `udp`, the following protocols are supported: `sctp`, `icmp`, `igmp`, `ipip`, `egp`, `pup`, `idp`, `tp`, `rsvp`, `gre`, `pim`, `esp`, `ah`, `mtp`, `encap`, `comp`, `ipv6`, `ospf`, `eigrp`, `isis`, `raw`, or other.

Related Information

- [Network Client Detection](#)
- [Pattern Matching](#)
- [Time Dependent Plugins](#)
- [Plugin Examples](#)



Network Client Detection

Match patterns that begin with the ^ symbol mean at least one line in the packet payload must begin with the following pattern. Match patterns that begin with the ! symbol indicate that the string must NOT match anything in the packet payload. In this case, the ! and ^ symbols are combined to indicate that Tenable Nessus Network Monitor should not evaluate any packet whose payload contains a line starting with the pattern Received: .

The ^ is more expensive to evaluate than the > symbol. So, while both match patterns ^<pattern> and ><pattern> would find <pattern> at the beginning of a packet payload, the use of > is more desirable as it is less costly. Use ^ when looking for the occurrence of a string at the beginning of a line, but not at the beginning of the packet payload. In the latter case, use the > character instead.

```
id=79526
hs_dport=25
clientissue
name=Buffer overflow in multiple IMAP clients
description=The remote e-mail client is Mozilla 1.3 or 1.4a which is vulnerable to a
boundary condition error whereby a malicious IMAP server may be able to crash or
execute code on the client.
solution=Upgrade to either 1.3.1 or 1.4a
risk=HIGH
match=^From:
match=^To:
match=^Date:
match=^User-Agent: Mozilla
match=!^Received:
regex=^User-Agent: Mozilla/.* \(.rv:(1\3|1\4a)
```




Pattern Matching

Tenable Nessus Network Monitor Can Match "Previous" Packets

Tenable Nessus Network Monitor allows matching on patterns in the current packet as well as patterns in the previous packet in the current session. This plugin shows how we can make use of this feature to determine if a Unix password file is sent by a web server:

```
id=79175
name>Password file obtained by HTTP (GET)
family=Generic
sport=80
description=It seems that a Unix password file was sent by the remote web server when
the following request was made :\n%P\nWe saw : \n%L
pmatch=>GET /
pmatch=HTTP/1.
match=root
match=daemon
match=bin
regex=root:.*:0:0:.*:.*
```

Here we see **match** patterns for a root entry in a Unix password file. We also see **pmatch** patterns that match against a packet that makes an HTTP GET request to a web server. The **match** patterns apply the current packet in a session and the **pmatch** patterns apply to the packet that was captured immediately before the one in the current session. To explain this visually, we are looking for occurrences of the following:

GET / HTTP/1.*

1) client -----> server:port 80

Contents of password file:

root:.*:0:0:.*:.*

2) client <----- server:port 80

Our **match** pattern would focus on the contents in packet 2) and our **pmatch** pattern would focus on packet 1) payload contents.

Tenable Nessus Network Monitor Can Match Binary Data



Tenable Nessus Network Monitor also allows matching against binary patterns. Here is an example plugin that makes use of binary pattern matching to detect the usage of the well-known community string “public” in SNMPv1 response packets (The “#” is used to denote a comment):

```
###
# SNMPv1 response
#
# Matches on the following:
# 0x30          - ASN.1 header
# 0x02 0x01 0x00 - (integer) (byte length) (SNMP version - 1)
# 0x04 0x06 public - (string) (byte length) (community string - "public")
# 0xa2          - message type - RESPONSE
# 0x02 0x01 0x00 - (integer) (byte length) (error status - 0)
# 0x02 0x01 0x00 - (integer) (byte length) (error index - 0)
###
id=71975
udp
sport=161
name=SNMP public community string
description=The remote host is running an SNMPv1 server that uses a well-known
community string - public
bmatch=>0:30
bmatch=>2:020100
bmatch=>5:04067075626c6963a2
bmatch=020100020100
```

Binary match patterns take the following form:

```
bmatch=[<>[off]:]<hex>
```

Binary match starts at <off>'th offset of the packet or at the last <offset> of the packet, depending on the use of > (start) or < (end). <hex> is a hex string we look for.

```
bmatch=<:ffffffff
```

This matches any packet whose last four bytes are set to 0xFFFFFFFF.

```
bmatch=>4:41414141
```

This matches any packet that contains the string “AAAA” (0x41414141 in hex) starting at its fourth byte.

```
bmatch=123456789ABCDEF5
```



This matches any packet that contains the hex string above.

Negative Matches

Tenable Nessus Network Monitor plugins can also be negated. Here are two examples:

```
pmatch=!pattern
```

```
pbmatch=>0: !414141
```

In each of these cases, the plugin does not match if the patterns contained in these “not” statements are present. For example, in the first `pmatch` statement, if the pattern named “pattern” is present, then the plugin does not match. In the second statement, the binary pattern of “AAA” (the letter “A” in ASCII hex is 0x41) only matches if it does not present the first three characters.



Time Dependent Plugins

The last plugin example shows some more advanced features of the Tenable Nessus Network Monitor plugin language that allows a plugin to be time dependent as well as make use of the evaluation of other plugins. The plugin shows how Tenable Nessus Network Monitor detects an anonymous FTP server. Use the **NEXT** keyword to separate plugins in the plugin file.

```
id=79200
nooutput
hs_sport=21
name=Anonymous FTP (login: ftp)
pmatch=^USER ftp
match=^331
NEXT #-----
id=79201
dependency=79200
timed-dependency=5
hs_sport=21
name=Anonymous FTP enabled
description=The remote FTP server has anonymous access enabled.
risk=LOW
pmatch=^PASS
match=^230
```

Since we want to detect an anonymous FTP server, we must look for the following traffic pattern:

USER ftp

1) FTP client -----> FTP server

331 Guest login ok, ...

2) FTP client <----- FTP server

PASS joe@fake.com

3) FTP client -----> FTP server

230 Logged in

4) FTP client <----- FTP server



Here we cannot use a single plugin to detect this entire session. So, instead we use two plugins: the first plugin looks for packets 1) and 2) and the second plugin looks for packets 3) and 4).

A review of the above plugin shows that plugin 79200 matches 1) and 2) in the session by keying on the patterns “USER ftp” and the 331 return code. Plugin 79201 matches on 3) and 4) by keying on the patterns “PASS” and the 230 return code.

Notice that plugin 79201 contains the following field: **dependency=79200**. This field indicates the plugin 79200 must evaluate successfully before plugin 79201 may be evaluated.

To complete the plugin for the anonymous FTP session, we must ensure both plugins are evaluating the same FTP session. To do this, we attach a time dependency to plugin 79201. The field **time-dependency=5** indicates that plugin 79200 must evaluate successfully in the last five seconds for 79201 to evaluate. This way, we can ensure that both plugins evaluate the same FTP session.



Plugin Examples

Basic Example

This plugin illustrates the basic concepts of Tenable Nessus Network Monitor plugin writing:

```
id=79873
nid=11414
hs_sport=143
name=IMAP Banner
description=An IMAP server is running on this port. Its banner is :\n %L
risk=NONE
match=OK
match=IMAP
match=server ready
regex=^.*OK.*IMAP.*server ready
```

This example uses the following fields:

- **id** - A unique number assigned to this plugin.
- **nid** - The Tenable Nessus ID of the corresponding Tenable Nessus NASL script.
- **hs_sport** - The source port to key on if High Performance mode is enabled.
- **name** - The name of the plugin.
- **description** - A description of the problem or service.
- **match** - The set of match patterns that must be found in the payload of the packet before the regular expression can be evaluated.
- **regex** - The regular expression to apply to the packet payload.

Tip: The description contains the %L macro. If this plugin evaluates successfully, then the string pattern in the payload that matched the regular expression is stored in %L and prints out at report time.

Complex Example

```
id=79004
nid=10382
```



```
cve=CVE-2000-0318
bid=1144
hs_sport=143
name=Atrium Mercur Mailserver
description=The remote imap server is Mercur Mailserver 3.20. There is a flaw in this
server (present up to version 3.20.02) which allow any authenticated user to read any
file on the system. This includes other user mailboxes, or any system file. Warning :
this flaw has not been actually checked but was deduced from the server banner
solution=There was no solution ready when this vulnerability was written; Please
contact the vendor for updates that address this vulnerability.
risk=HIGH
match=>* OK
match=MERCUR
match=IMAP4-Server
regex=^\>* OK.*MERCUR IMAP4-Server.*v3\.20\..*$
```

Tip: The first match pattern makes use of the > symbol. The > symbol indicates that the subsequent string must be at the beginning of the packet payload. Use of the > symbol is encouraged where possible as it is an inexpensive operation.

Case-Insensitive Example

There is a tool called **SmartDownloader** that uploads and downloads large files. Unfortunately, versions 0.1 through 1.3 use the capitalization **SmartDownloader**, versions 1.4 through 2.7 use **smartdownloader** and versions 2.8 through current use **SMARTdownloader**. Searching for the various combinations of this text with purely the **regex** command would cause us to use a statement that looks like this:

```
regex=[sS][mM][aA][rR][tT][dD]own[lL]oader
```

However, with the **regexi** command, the search string is much less complex and less prone to creating an error:

```
regexi=smartdownloader
```

By using **regexi**, we can more quickly match on all three versions as well as future permutations of the string **smartdownloader**. In a case such as this, **regexi** is the logical choice.

```
id=79910
```



```
dependency=1442
hs_sport=6789
name=SmartDownloader Detection
description=The remote host is running SmartDownloader, a tool for performing
rudimentary uploads and downloads of large binary files.
solution=Ensure that this application is in keeping with Corporate policies and
guidelines
risk=MEDIUM
family=PeerToPeer
match=ownloader
regexi=smartdownloader
```

Above is a complete example Tenable Nessus Network Monitor plugin using the **regexi** keyword. The use of the **match** keyword searching for the string **ownloader** is not a typo. By searching for network sessions that have this string in them first, Tenable Nessus Network Monitor can avoid invoking the expensive **regexi** search algorithm unless the **ownloader** pattern is present.



Tenable Nessus Network Monitor Real-Time Plugin Syntax

Real-Time Plugin Model

Tenable Nessus Network Monitor real-time plugins are exactly the same as Tenable Nessus Network Monitor vulnerability plugins with two exceptions:

- They can occur multiple times.
- Their occurrence may not be recorded as a vulnerability.

For example, an attacker may attempt to retrieve the source code for a Perl script from an Apache web server. If Tenable Nessus Network Monitor observes this event, it would be logical to send a real-time alert. It would also be logical to mark that the Apache server is potentially vulnerable to some sort of Perl script source code download. In other cases, it may be more logical to just log the attempt as an event, but not a vulnerability. For example, a login failure over FTP is an event that may be worth logging, but does not indicate a vulnerability.

As the real-time plugins are written, there are two keywords that indicate to Tenable Nessus Network Monitor that these are not regular vulnerability plugins. These are the **real-time** and **realtimeonly** keywords.

In the previous example, the FTP user login failure would be marked as a **realtimeonly** event because we would like real-time alerting, but not a new entry into the vulnerability database.

Real-Time Plugin Keywords

Name	Description
<code>real-time</code>	If a plugin has this keyword, then Tenable Nessus Network Monitor will generate a SYSLOG message or real-time log file entry the first time this plugin matches. This prevents vulnerabilities that are worm related from causing millions of events. For example, the plugins for the Sasser worm generate only one event. Output from plugins with this keyword will show up in the vulnerability report.
<code>realtimeonly</code>	If a plugin has this keyword, then Tenable Nessus Network Monitor will generate a SYSLOG message or real-time log file entry each time the plugin evaluates successfully. These plugins never show up in the



Name	Description
	report file.
track-session	This keyword will cause the contents of a session to be reported (via SYSLOG or the real-time log file) a specified number of times after the plugin containing this keyword was matched. This is an excellent way to discover what a hacker “did next” or possibly what the contents of a retrieved file were real-time.
trigger-dependency	Normally if a plugin has multiple dependencies, then all of those dependencies must be successful for the current plugin to evaluate. However, the trigger-dependency keyword allows a plugin to be evaluated as long as at least one of its dependencies is successful.



Real-Time Plugin Examples

Failed Telnet Login Plugin

The easiest way to learn about Tenable Nessus Network Monitor real-time plugins is to evaluate some of those included by Tenable. Below is a plugin that detects a failed Telnet login to a FreeBSD server.

```
# Look for failed logins into an FreeBSD telnet server
id=79400
hs_sport=23
dependency=1903
realtimeonly
name=Failed login attempt
description=Tenable Nessus Network Monitor detected a failed login attempt to a telnet
server
risk=LOW
match=Login incorrect
```

This plugin has many of the same features as a vulnerability plugin. The ID of the plugin is 79400. The high-speed port is 23. We need to be dependent on plugin 1903 (which detects a Telnet service). The **realtimeonly** keyword tells Tenable Nessus Network Monitor that if it observes this pattern, then it should alert on the activity, but not record any vulnerability.

In Tenable Security Center, events from Tenable Nessus Network Monitor are recorded alongside other IDS tools.

Finger User List Enumeration Plugin

The **finger** daemon is an older Internet protocol that allowed system users to query remote servers to get information about a user on that box. There have been several security holes in this protocol that allowed an attacker to elicit user and system information that could be useful to attackers.

```
id=79500
dependency=1277
hs_sport=79
track-session=10
realtimeonly
```



```
name=App Subversion - Successful finger query to multiple users
description=A response from a known finger daemon was observed which indicated that the
attacker was able to retrieve a list of three or more valid user names.
risk=HIGH
match=Directory:
match=Directory:
match=Directory:
```

This plugin looks for these patterns only on systems where a working **finger** daemon has been identified (dependency #1277). However, the addition of the **track-session** keyword means that if this plugin is launched with a value of 10, the session data from the next 10 packets is tracked and logged in either the SYSLOG or real-time log file.

During a normal finger query, if only one valid user is queried, then only one home directory is returned. However, many of the exploits for finger involve querying for users such as *NULL*, ..., or 0. This causes vulnerable **finger** daemons to return a listing of all users. In that case, this plugin would be activated because of the multiple “Directory:” matches.

Unix Password File Download Web Server Plugin

This plugin below looks for any download from a web server that does not look like HTML traffic, but does look like the contents of a generic Unix password file.

```
id=79300
dependency=1442
hs_sport=80
track-session=10
realtimeonly
name=Web Subversion - /etc/passwd file obtained
description=A file which looks like a Linux /etc/passwd file was downloaded from a web
server.
risk=HIGH
match=!<HTML>
match=!<html>
match=^root:x:0:0:root:/root:/bin/bash
match=^bin:x:1:1:bin:
match=^daemon:x:2:2:daemon:
```



The plugin is dependent on Tenable Nessus Network Monitor ID 1442, which detects web servers. In the match statements, we attempt to ignore any traffic that contains valid HTML tags, but also has lines that start with common Unix password file entries.

Generic Buffer Overflow Detection on Windows Plugin

One of Tenable Nessus Network Monitor's strongest intrusion detection features is its ability to recognize specific services, and then to look for traffic occurring on those services that should never occur unless they have been compromised. Since Tenable Nessus Network Monitor can keep track of both sides of a conversation and make decisions based on the content of each, it is ideal to look for Unix and Windows command shells occurring in services that should not have those command shells in them. Here is an example plugin:

```
# look for Windows error when a user tries to
# switch to a drive that doesn't exist
id=79201
include=services.inc
trigger-dependency
track-session=10
realtimeonly
name=Successful shell attack detected - Failed cd command
description=The results of an unsuccessful attempt to change drives on a Windows
machine occurred in a TCP session normally used for a standard service. This may
indicate a successful compromise of this service has occurred.
risk=HIGH
pmatch=!>GET
pregexi=cd
match=!>550
match=^The system cannot find the
match=specified.
```

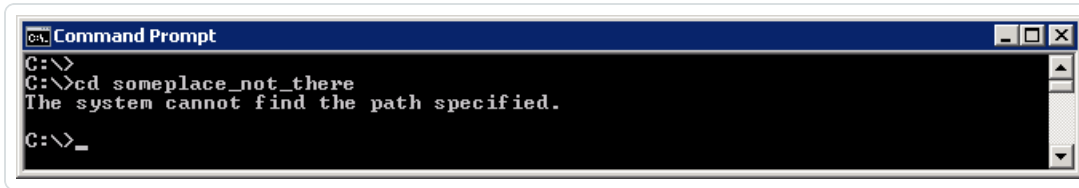
This plugin uses the **include** keyword that identifies a file that lists several dozen Tenable Nessus Network Monitor IDs, which identify well known services such as HTTP, DNS, and NTP. The plugin is not evaluated unless the target host is running one of those services.

The keyword **trigger-dependency** is needed to ensure the plugin is evaluated even if there is only one match in the **services.inc** file. Otherwise, Tenable Nessus Network Monitor evaluates this plugin only if the target host was running all Tenable Nessus Network Monitor IDs present in the



`services.inc` file. The `trigger-dependency` keyword says that at least one Tenable Nessus Network Monitor ID must be specified by one or more dependency or include rules must be present.

Finally, the logic of plugin detection looks for the following type of response on a Windows system:



```
Command Prompt
C:\>
C:\>cd someplace_not_there
The system cannot find the path specified.
C:\>_
```

In this case, a user has attempted to use the `cd` command to change directories within a file system and the attempt was not allowed. This is a common event that occurs when a remote hacker compromises a Windows 2000 or Windows 2003 server with a buffer overflow. The Tenable Nessus Network Monitor plugin looks for a network session that should not be there.

In the plugin logic, there are `pmatch` and `pregexi` statements that attempt to ensure that the session is not an HTTP session, and that the previous side of the session contains the string `cd`.

Tip: The `pregexi` statement could be expanded to include the trailing space after the “d” character and also the first character.

The plugin then looks for the expected results of the failed `cd` command. The first match statement makes sure this pattern is not part of the FTP protocol. Looking for “cd” in one side of a session and the error of attempting to change to a directory in an FTP session causes false positives for this plugin. Adding a rule to ignore if a line starts with “550” avoids this. While writing and testing this plugin, Tenable considered having a different set of plugins just for FTP, but the additional filter statement took care of any false positives. Finally, the last two match statements look for the results of the failed change directory attempt. They are spread across two match statements and could have been combined into one regular expression statement, but there was enough content in the basic message to split them into higher-speed matching.



Tenable Nessus Network Monitor Corporate Policy Plugins

Most companies have an “Acceptable Use Policy” that defines appropriate use of the company’s IT facilities. Often, this policy is abused to some extent since detecting abuse can be difficult.

Tenable Nessus Network Monitor can help in this regard through use of Tenable Nessus Network Monitor Corporate Policy plugins. These plugins can be used to look for policy violations and items such as credit card numbers, Social Security numbers, and other sensitive content in motion.

Tenable ships Tenable Nessus Network Monitor with a large number of plugins that are frequently updated. The primary focus of these plugins is to discover hosts, applications and their related client/server vulnerabilities. To search for a specific plugin, visit <http://www.tenable.com/NNM-plugins>.

Many of the available plugins already detect activities that would fall into the “Inappropriate Use” category in most companies. Some of the activities that are detected through these plugins include (but are not limited to):

- Game servers
- Botnet clients and servers
- Peer to peer file sharing
- IRC clients and servers
- Chat clients
- Tunneling software or applications like Tor, GoToMyPC, and LogMeIn

Related Information

- [Detecting Custom Activity Prohibited by Policy](#)
- [Detecting Confidential Data in Motion](#)



Detecting Custom Activity Prohibited by Policy

The plugins provided with Tenable Nessus Network Monitor are useful for detecting generally inappropriate activities, but there may be times when more specific activities need to be detected. For example, a company may want to generate an alert when email is sent to a competitor's mail service or if users are managing their Facebook accounts from the corporate network.

Tenable provides the ability for users to write their own custom plugins, as documented in [Tenable Nessus Network Monitor Plugin Syntax](#). These plugins are saved as `prn` files.

The following example shows how to create a custom plugin to detect users logging into their Facebook accounts. First, a unique plugin ID is assigned, in this case `79420`. So, the first line of our plugin is:

```
id=79420
```

Next, we want a description of what the vulnerability detects:

```
description=The remote client was observed logging into a Facebook account.
You should ensure that such behavior is in alignment with corporate policies
and guidelines. For your information, the user account was logged as:\n %L
```

The `%L` is the results of our regular expression statement that is created later. We want to log the source address of the offending computer as well as the user ID that was used to log in. Next, we create a distinct name for our plugin.

```
name=POLICY - Facebook usage detection
```

Note that the name begins with the string `POLICY`. This makes all `POLICY` violations easily searchable from the Tenable Security Center interface.

You can also define a Tenable Security Center dynamic asset that contains only `POLICY` violators.

The next field defines a family. For this example, the application is a web browser, so the family ID is defined as follows:

```
family=Web Clients
```

Since this is a web browser, a dependency can be assigned that tells Tenable Nessus Network Monitor to look at only those clients that have been observed surfing the web:

```
dependency=1735
```




Furthermore, since we are looking at client traffic, we define:

```
clientissue
```

Next, we assign a risk rating for the observed behavior:

```
risk=MEDIUM
```

In the final section we create **match** and **regex** statements that Tenable Nessus Network Monitor looks for passively. We want all of these statements to be true before the client is flagged for inappropriate usage:

```
match=>POST /
```

The web request must begin with a POST verb. This weeds out all “GET” requests.

```
match=^Host: *.facebook.com
```

The statement above ensures that they are posting a host with a domain of *.facebook.com.

Finally, we have a **match** and **regex** statement that detects the user’s login credentials:

```
match=email=
```

```
regex=email=.*%40[^&]+
```

Altogether, we have a single plugin as follows:

```
id=79420
family=Web Clients
clientissue
dependency=1735
name=Facebook_Usage
description=The remote client was observed logging into a Facebook account.
You should ensure that such behavior is in alignment with
Corporate Policies and guidelines. For your information, the user account
was logged as:
risk=MEDIUM
solution=Stay off of Facebook.
match=>POST /
match=^Host: *.facebook.com
match=email=
regex=email=.*%40[^&]+
```



This plugin could be named **Facebook.prm** and added into the `/opt/nnm/var/nnm/plugins/` directory. If Tenable Security Center is used to manage one or more Tenable Nessus Network Monitor systems, use the plugin upload dialog to add the new `.prm` file.

If you wish to create a policy file that includes multiple checks, use the reserved word *NEXT* within the policy file. For example:

```
id=79420
...
rest of plugin
...
NEXT
id=79421
...
etc.
```



Detecting Confidential Data in Motion

Many organizations want to ensure that confidential data does not leave the network. Tenable Nessus Network Monitor can aid in this by looking at binary patterns within observed network traffic. If critical documents or data can be tagged with a binary string, such as an MD5 checksum, Tenable Nessus Network Monitor has the ability to detect these files being passed outside the network. For example:

Create a document that has a binary string of:

0xde1d7f362734c4d71ecc93a23bb5dd4c and 0x747f029fbf8f7e0ade2a6198560c3278

A Tenable Nessus Network Monitor plugin can then be created to look for this pattern as follows:

```
id=79580
trigger-dependency
dependency=2004
dependency=2005
hs_dport=25
description=POLICY - Confidential data passed outside the
corporate network. The Confidential file don'tshare.doc was
just observed leaving the network via email.
name=Confidential file misuse
family=Generic
clientissue
risk=HIGH
bmatch=de1d7f362734c4d71ecc93a23bb5dd4c
bmatch=747f029fbf8f7e0ade2a6198560c3278
```

These binary codes were created by simply generating md5 hashes of the following strings:

```
"Copyright 2006 BigCorp, file: don'tshare.doc"
```

```
"file: don'tshare.doc"
```

The security compliance group maintains the list of mappings (confidential file to md5 hash). The md5 hash can be embedded within the binary file and can then be tracked as it traverses the network.



Similar checks can be performed against ASCII strings to detect, for example, if confidential data was cut-and-pasted into an email. Simply create text watermarks that appear benign to the casual observer and map to a specific file name. For example:

"Reference data at \\192.168.0.2\c\$\shares\employmentfiles for HR data regarding Jane McIntyre" could be a string which maps to a file named Finances.xls.

A Tenable Nessus Network Monitor plugin can look for the string as follows:

```
id=79581
trigger-dependency
dependency=2004
dependency=2005
hs_dport=25
description=POLICY - Confidential data passed outside the
corporate network. Data from the confidential file Finances.xls was just
observed leaving the network via email.
name=Confidential file misuse
family=Generic
clientissue
risk=HIGH
match=Reference data at
match=192.168.0.2\c$\shares\employmentfiles
match=for HR data regarding Jane McIntyre
```

The two example plugins above (IDs 79580 and 79581) detect files leaving the network via email. Most corporations have a list of ports that are allowed outbound access. SMTP is typically one of these ports. Other ports may include FTP, Messenger client ports (e.g., AIM, Yahoo and ICQ), or Peer2Peer (e.g., GNUTELLA and BitTorrent). Depending on your specific network policy, you may wish to clone plugins 79580 and 79581 to detect these strings on other outbound protocols.



Internal Tenable Nessus Network Monitor Plugin IDs

Each vulnerability and real-time check Tenable Nessus Network Monitor performs has a unique associated ID. Tenable Nessus Network Monitor IDs are within the range 0 to 10000.

Internal Tenable Nessus Network Monitor IDs

Some of Tenable Nessus Network Monitor's checks, such as detecting open ports, are built in. The following chart lists some of the more commonly encountered internal checks and describes what they mean:

NNM ID	Name	Description
0	Detection of Open Port	Tenable Nessus Network Monitor has observed a SYN-ACK leave from a server.
1	Operating System Fingerprint	Tenable Nessus Network Monitor has observed enough traffic about a server to guess the operating system.
2	Service Connection	Tenable Nessus Network Monitor has observed browsing traffic from a host.
3	Internal Client Trusted Connections	Tenable Nessus Network Monitor has logged a unique network session of source IP, destination IP, and destination port.
4	Internal Interactive Session	Tenable Nessus Network Monitor has detected one or more interactive network sessions between two hosts within your focus network.
5	Outbound Interactive Sessions	Tenable Nessus Network Monitor has detected one or more interactive network sessions originating from within your focus network and destined for one or more addresses on the Internet.
6	Inbound Interactive Sessions	Tenable Nessus Network Monitor has detected one or more interactive network sessions ori-



NNM ID	Name	Description
		ginating from one or more addresses on the Internet to this address within your focus network.
7	Internal Encrypted Session	Tenable Nessus Network Monitor has detected one or more encrypted network sessions between two hosts within your focus network.
8	Outbound Encrypted Session	Tenable Nessus Network Monitor has detected one or more encrypted network sessions originating from within your focus network and destined for one or more addresses on the Internet.
9	Inbound Encrypted Session	Tenable Nessus Network Monitor has detected one or more encrypted network sessions originating from one or more addresses on the Internet to this address within your focus network.
12	Number of Hops	Tenable Nessus Network Monitor logs the number of hops away each host is located.
14	Accepts External Connections	Tenable Nessus Network Monitor detects an external connection to this host. Specific IP addresses are not reported by this plugin, but it does track the destination port and protocol used. You can view full connection details in the real-time event log. This is the opposite of plugin 16, which reports on outbound connections.
15	Internal Server Trusted Connections	Tenable Nessus Network Monitor has logged a unique network session of source IP, destination IP, and destination port. Specific IP addresses are not reported by this plugin, but it does track which destination port and protocol was used. You can view full connection details in the real-time event log. This is the opposite of plugin 14,



NNM ID	Name	Description
		which reports on inbound connections.
16	Outbound External Connection	Tenable Nessus Network Monitor has detected an external connection from this host.
17	TCP Session	Tenable Nessus Network Monitor identifies TCP sessions and reports the start time, number of bytes of data downloaded during, and end time of these sessions. This plugin is reported at the end of each TCP session.
18	IP Protocol Detection	Tenable Nessus Network Monitor detects all IP protocols.
19	VLAN ID Reporting	Tenable Nessus Network Monitor reports all observed VLAN tags per host.
20	IPv6 Tunneling	Tenable Nessus Network Monitor identifies and processes tunneled IPv6 traffic.



Real-Time Traffic Analysis Configuration Theory

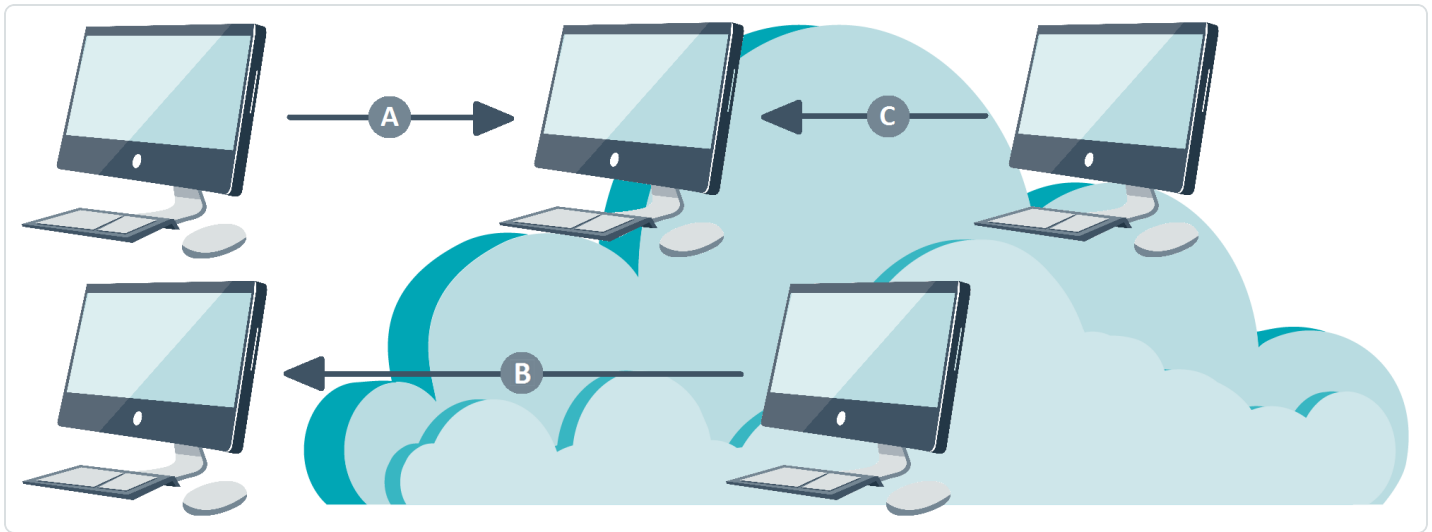
This section describes how configuration options affect Tenable Nessus Network Monitor operation and provides the following details on Tenable Nessus Network Monitor architecture:

- [Focus Network](#)
- [Detecting Server and Client Ports](#)
- [Detecting Specific Server and Client Port Usage](#)
- [Firewall Rules](#)
- [Working with Tenable Security Center](#)
- [Selecting Rule Libraries and Filtering Rules](#)
- [Detecting Encrypted and Interactive Sessions](#)
- [Routes and Hop Distance](#)
- [Alerting](#)



Focus Network

When a focus network is specified via the Monitored Networks IP Addresses and Ranges configuration parameter, only one side of a session must match in the list. For example, if you have a DMZ that is part of the focus network list, Tenable Nessus Network Monitor reports on vulnerabilities of the web server there, but not on web clients visiting from outside the network. However, a web browser within the DMZ visiting the same web server is reported.



In the diagram above, three sessions labeled A, B, and C are shown communicating to, from, and inside a focus network. In session A, Tenable Nessus Network Monitor analyzes only those vulnerabilities observed on the server inside the focus network and does not report client side vulnerabilities. In session B, Tenable Nessus Network Monitor ignores vulnerabilities on the destination server, but reports client side vulnerabilities. In session C, both client and server vulnerabilities are reported.

There is another filter that Tenable Nessus Network Monitor uses while looking for unique sessions. This is a dependency that requires the host to run a major service. These dependencies are defined by a list of Tenable Nessus Network Monitor plugin IDs that identify SSL, FTP, and several dozen other services.

Finally, the entire process of detecting these sessions can be filtered by specific network ranges and ports. For example, if a University ran a public FTP server that had thousands of downloads each hour, they may want to disable interactive sessions on port 21 on that FTP server. Similarly, disabling encryption detection on ports such as 22 and 443 also eliminates some noise for Tenable Nessus Network Monitor.



Detecting Server and Client Ports

The method used by TCP connections to initiate communication is known as the “three-way handshake.” This method can be compared to how a common telephone conversation is initiated. If Bob calls Alice, he has effectively sent her, in TCP terms, a “SYN” packet. She may or may not answer. If Alice answers, she has effectively sent a “SYN-ACK” packet. The communication is still not established, since Bob may have hung up as she was answering. The communication is established when Bob replies to Alice, sending her an “ACK.”

The Tenable Nessus Network Monitor configuration option “connections to services” enables Tenable Nessus Network Monitor to log network client to server activity.

Whenever a system within the monitored network range tries to connect to a server over TCP, the connecting system emits a TCP “SYN” packet. If the port the client connects on is open, then the server responds with a TCP “SYN/ACK” packet. At this point, Tenable Nessus Network Monitor records both the client address and the server port the client connects to. If the port on the server is not open, then the server does not respond with a TCP “SYN/ACK” packet. In this case, since Tenable Nessus Network Monitor never sees a TCP “SYN/ACK” response from the server, Tenable Nessus Network Monitor does not record the fact that the client tried to connect to the server port, since the port is not available to that client.

The **Connections to Services** configuration parameter does not track how many times the connection was made. If the same host browses the same web server a million times, or browses a million different web servers once, the host is still marked as having browsed on port 80. This data is logged as Tenable Nessus Network Monitor internal plugin ID 2.

Tenable Nessus Network Monitor detects many applications through plugin and protocol analysis. At a lower level, Tenable Nessus Network Monitor also detects open ports and outbound ports in use on the monitored networks. By default, Tenable Nessus Network Monitor detects any TCP server on the protected network if it sees a TCP “SYN-ACK” packet.

In combination, the detection of server ports and client destination ports allows a network administrator to see who on their network is serving a particular protocol and who on their network is speaking that protocol.



Detecting Specific Server and Client Port Usage

The **Show Connections** configuration parameter keeps track of host communication within the focus network. When the **Show Connections** configuration parameter is enabled, if one of the hosts is in the defined focus network, Tenable Nessus Network Monitor records the client, server, and server port every time a host connects to another host. It does not track the frequency or time stamp of the connections - just that a connection was made.

The **Show Connections** configuration parameter provides a greater level of detail than the **Connections to Services** configuration parameter. For example, if your IPv4 address is 1.1.1.1 or your IPv6 address is 2001:DB8::AE59:3FC2 and you use the SSH service to connect to “some_company.com”, then the use of these options records the following:

Show Connections

```
some_company.com:SSH
```

```
2001:DB8::AE59:3FC2 -> some_company.com
```

Connections to Services

```
SSH
```

```
2001:DB8::AE59:3FC2 -> SSH
```

Using the **Connections to Services** configuration parameter lets you know that the system at 1.1.1.1 and 2001:DB8::AE59:3FC2 uses the SSH protocol. This information may be useful regardless of where the service is used.

Tenable Nessus Network Monitor does not log a session-by-session list of communications. Instead, it logs the relationship between the systems. For example, if system A is detected using the SSH protocol on port 22 connecting to system B, and both systems are within the focus network, Tenable Nessus Network Monitor would log:



- System A browses on port 22
- System B offers a service (listens) on port 22
- System A communicates with System B on port 22

If system B were outside of the focus network, Tenable Nessus Network Monitor would not record anything about the service system B offers, and would also log that system A browses outside of the focus network on port 22. Tenable Nessus Network Monitor does not log how often a connection occurs, only that it occurred at least once. For connections outside of the focus network, Tenable Nessus Network Monitor logs only which ports are browsed, not the actual destinations.

Note: If logging session-by-session network events is a requirement for your network analysis, Tenable offers the Tenable Log Correlation Engine product, which can log firewall, web server, router, and sniffer logs.



Firewall Rules

If Tenable Nessus Network Monitor is placed immediately behind a firewall such that all of the traffic presented to Tenable Nessus Network Monitor flows through the firewall, then the list of served ports, client side ports, and the respective IP addresses of the users are readily available.

Tools such as the Tenable Security Center Vulnerability Analysis page allow information about these ports (both client and server) to be browsed, sorted, and reported on. You can also view lists of IP addresses and networks using these client and server ports.



Working with Tenable Security Center

When Tenable Security Center manages multiple Tenable Nessus Network Monitor sensors, users of Tenable Security Center can analyze the aggregate types of open ports, browsed ports, and communication activity that occurs on the focus network. Since Tenable Security Center has several different types of users and privileges, many different IT and network engineering accounts can be created across an enterprise so they can share and benefit from the information detected by Tenable Nessus Network Monitor.



Selecting Rule Libraries and Filtering Rules

Tenable ships an encrypted library of passive vulnerability detection scripts. This file cannot be modified by the end users of Tenable Nessus Network Monitor. However, if certain scripts must be disabled, they can be specified by the PASL ID and “.pasl” appended. For example, *1234.pasl*, disables the PASL with the ID of 1234 on a single line in the **disabled-scripts.txt** file.

If a plugin must be disabled, type its ID on a single line in the **disabled-plugins.txt** file. If a plugin must be real-time enabled, type its ID on a single line in the **realtime-plugins.txt** file.

When adding Tenable Nessus Network Monitor plugins to the disabled plugin list, be sure to leave an empty blank line after typing the last plugin to be disabled. Failure to return to the next line can result in a non-functional disabled plugin list.

Example: 1234 [return]

If any of the referenced files do not exist, create them using the appropriate method for the operating system. The file locations are as follows:

Operating System	File Path
Linux	<code>/opt/nnm/var/nnm</code>
Windows	<code>C:\ProgramData\Tenable\NNM\nnm</code>
macOS	<code>/Library/NNM/var/nnm</code>



Detecting Encrypted and Interactive Sessions

Tenable Nessus Network Monitor can be configured to detect both encrypted and interactive sessions. An encrypted session is a TCP or UDP session that contains sufficiently random payloads. An interactive session uses timing and statistical profiling of the packets in a session to determine if the session involves human input at a command line prompt.

In both cases, Tenable Nessus Network Monitor identifies these sessions for the given port and IP protocol. It then lists the detected interactive or encrypted session as vulnerabilities.

Tenable Nessus Network Monitor has a variety of plugins to recognize telnet, Secure Shell (SSH), Secure Socket Layer (SSL), and other protocols. Combined with the detection of the interactive and encryption algorithms, Tenable Nessus Network Monitor may log multiple forms of identification for the detected sessions.

For example, Tenable Nessus Network Monitor may recognize not only an SSH service running on a high port as an encrypted session, but also recognize the version of SSH and determine any vulnerabilities associated with it.



Routes and Hop Distance

For active scans, one host can find the default route and an actual list of all routers between it and a target platform. To do this, it sends one packet after another with a slightly larger TTL (time to live) value. Each time a router receives a packet, it decrements the TTL value and sends it on. If a router receives a packet with a TTL value of one, it sends a message back to the originating server stating that the TTL has expired. The server sends packets to the target host with greater and greater TTL values and collects the IP addresses of the routers sending expiration messages in-between.

Since Tenable Nessus Network Monitor is entirely passive, it cannot send or elicit packets from the routers or target computers. It can however, record the TTL value of a target machine. The TTL value is an 8-bit field, which means it can contain a value between 0 and 255. Most machines use an initial TTL value of 32, 64, 128, or 255. Since there is a maximum of 16 hops between your host and any other host on the internet, Tenable Nessus Network Monitor uses an algorithm to map any TTL to the number of hops.

For example, if Tenable Nessus Network Monitor sniffed a server sending a packet with a TTL of 126, it detects that 128 is two hops away. Tenable Nessus Network Monitor does not know the IP address of the in-between routers.

Note: Modern networks have many devices such as NAT firewalls, proxies, load balancers, intrusion prevention, routers, and VPNs that rewrite or reset the TTL value. In these cases, Tenable Nessus Network Monitor may report inconsistent hop counts.



Alerting

When Tenable Nessus Network Monitor detects a real-time event, it can:

- Send the event to a local log file.
- Send the event via Syslog to a log aggregator such as Tenable Log Correlation Engine, an internal log aggregation server.
- Send the event to a third party security event management vendor.

New Host Alerting

You can configure Tenable Nessus Network Monitor to detect when a new host has been added to the network. By default, Tenable Nessus Network Monitor has no knowledge of your network's active hosts, so the first packets Tenable Nessus Network Monitor sniffs trigger an alert. To avoid this, you can configure Tenable Nessus Network Monitor to learn the network over a period of days. Once this period is over, any "new" traffic must be from a host that has not communicated during the initial training.

To prevent Tenable Nessus Network Monitor from triggering new host alerts on known hosts, you can create a known hosts file in the location to which the Known Hosts File configuration parameter is set. Each line of the Known

Hosts File supports a single IPv4 or IPv6 address. Hyphenated ranges and CIDR notation are not supported. Tenable Nessus Network Monitor must be restarted after creating or making any changes to the Known Hosts File.

When Tenable Nessus Network Monitor logs a new host, the Ethernet address saves in the message. When Tenable Nessus Network Monitor is more than one hop away from the sniffed traffic, the Ethernet address is that of the local switch and not the actual host. If the scanner is deployed in the same collision domain as the sniffed server, then the Ethernet address is accurate.

For DHCP networks, Tenable Nessus Network Monitor often detects a "new" host. Tenable® recommends deploying this feature on non-volatile networks such as DMZ. Users should also consider analyzing Tenable Nessus Network Monitor "new" host alerts with Tenable Security Center, which can sort real-time Tenable Nessus Network Monitor events by networks.



Syslog Messages

Tenable Nessus Network Monitor provides options to send real-time and vulnerability data as Syslog messages. This section describes the available Syslog message types:

- [Standard Syslog Message Types](#)
- [CEF Syslog Message Types](#)



Standard Syslog Message Types

Message Types

- Syslog message format for real-time Syslog entries generated by realtimeonly PRMs:

```
<priority>timestamp nnm: src_ip:src_port|dst_ip:dst_port|protocol|plugin_id|plugin_name|matched_text_current_packet|matched_text_previous_packet|risk
```

- Syslog message format for vulnerability and real-time Syslog entries generated by PASLs, PRMs, and internal plugins:

```
<priority>timestamp nnm: src_ip:src_port|dst_ip:dst_port|protocol|plugin_id|plugin_name|plugin_description|plugin_output|risk
```

Message Fields

Name	Description
dst_ip	Displays the destination IP address for reported traffic.
dst_port	Displays the destination port for reported traffic.
matched_text_current_packet	Reports the payload, causing a match in the packet to trigger the Tenable Nessus Network Monitor event.
matched_text_previous_packet	Reports the payload that was observed prior to the payload in the matched_text_current_packet field.
plugin_id	Displays the reported Tenable Nessus Network Monitor plugin or PASL ID triggered by reported traffic.
plugin_name	Displays the name of the Tenable Nessus Network Monitor plugin or PASL ID triggered by reported traffic.
plugin_output	Displays dynamic data for a given vulnerability or event. This field may be empty if there is no plugin-specific data.



Name	Description
priority	Displays the Syslog facility level of the message.
protocol	Reports the integer value for the protocol used for the reported traffic.
risk	Displays the associated risk level of the reported vulnerability. This can be NONE , LOW , MEDIUM , HIGH , CRITICAL , or INFO .
src_ip	Displays the source IP address reported for the traffic.
src_port	Displays the source port for the reported traffic.
timestamp	Displays the date and time of the Syslog message.



CEF Syslog Message Types

Message Type

Syslog message format for vulnerability and real-time Syslog entries generated by PASLs, PRMs, and internal plugins:

```
timestamp CEF: Version|Device Vendor|Device Product|Device Version|Signature  
ID|Name|Severity|Extension
```

Message Fields

Name	Description
Device Product	Displays the name of the product on the detected sending device.
Device Vendor	Displays the vendor of the product on the detected sending device.
Device Version	Displays the version of the product on the detected sending device.
Extension	Displays key-value pairs for one or more of the following additional fields: src, dst, spt, dpt, proto, and msg.
Name	Displays the name of the Tenable Nessus Network Monitor plugin or PASL ID triggered by the reported traffic.
Severity	Displays the associated severity level of the reported vulnerability.
Signature ID	Displays the reported Tenable Nessus Network Monitor plugin or PASL ID triggered by the reported traffic.
timestamp	Displays the date and time of the Syslog message.
Version	Displays the version of the CEF format version.



Unknown or Customized Ports

Many networks contain traffic on ports Tenable Nessus Network Monitor defines as different traffic types or alternate ports. If the port is not defined, it displays as **Unknown**. The **NNM-services** file may be edited to either customize or add the port information to provide accurate reporting for ports on the network.

For example, by default, there are two lines in the **NNM-services** file that define SMTP traffic. They read `smtp 25/tcp` and `smtp 25/udp`. If the organization routinely sends SMTP data over port 2525 those lines can be updated to read `smtp 2525/tcp` and `smtp 2525/udp`.



Working with Tenable Security Center

Tenable Nessus Network Monitor can operate under the control of Tenable Security Center, which provides Tenable Nessus Network Monitor with passive vulnerability data and retrieves scanned data. Tenable Security Center has a variety of reporting, remediation, and notification mechanisms to efficiently distribute vulnerability information across large enterprises. In addition, it can also control a distributed set of Tenable Nessus active vulnerability scanners. By combining active and passive vulnerability scanning, Tenable Security Center can be used to efficiently and accurately manage security across large networks.

This section contains the following information about Tenable Nessus Network Monitor integration with Tenable Security Center.

- [Managing Vulnerabilities](#)
- [Updating the Tenable Nessus Network Monitor Management Interface](#)



Managing Vulnerabilities

Tenable Security Center displays a summary of vulnerabilities detected by Tenable Nessus Network Monitor. These vulnerabilities can be independently viewed by many different users with different access control. Tenable Security Center also allows security managers to issue recommendations that help guide network administrators as to which vulnerabilities should be mitigated.

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

Vulnerability Analysis Options

Filters ←

Vulnerability List ▼ Jump to Vulnerability Detail List
Total Results: 56

Plugin ID	Name	Family	Severity	IP Address
801013	Safari < 5.0.4 Multiple Vulnerabilities	Web Clients	High	10.3
801014	Mac OS X : Safari < 6.0.5 Multiple Security Vulnerabilities	Web Clients	Medium	10.3
801012	Safari < 4.1 / 5.0 Multiple Vulnerabilities	Web Clients	High	10.3
800102	Safari Version Detection	Web Clients	Info	10.3
801019	Safari < 3.2 Multiple Vulnerabilities	Web Clients	High	10.3
801011	Safari < 3.2.2 Multiple Vulnerabilities	Web Clients	High	10.3
800035	Web Access Statistics	Generic	Info	10.3
801014	Mac OS X : Safari < 6.0.5 Multiple Security Vulnerabilities	Web Clients	Medium	10.3
801009	Safari < 4.0.5 Multiple Vulnerabilities	Web Clients	High	10.3
800000	Host Discovered	Generic	Info	10.3
800036	Web Error Statistics	Generic	Info	10.3

Filters:

- Address: 10.3
- Plugin Name: All
- Severity: All

Actions: Select Filters, Clear Filters, Load Query

Tenable Nessus Network Monitor is Real-Time

Since Tenable Nessus Network Monitor’s vulnerability data is constantly fed into Tenable Security Center and Tenable Nessus Network Monitor’s plugins are updated by Tenable®, the accuracy of the passive vulnerability data in Tenable Security Center greatly enhances the quality of the security information available to Tenable Security Center users.



Offline Tenable Nessus Network Monitor Plugin Update in Tenable Security Center

To perform an offline Tenable Nessus Network Monitor plugin update:

1. If not already in place, install a Tenable Nessus Network Monitor scanner on the same host as Tenable Security Center. It does not need to be started or otherwise configured.
2. To prevent the Tenable Nessus Network Monitor scanner from starting automatically upon restarting the system, run the following command:

```
# /sbin/systemctl is-enabled nnm off
```

3. Run the following command and save the challenge string that is displayed:

```
# /opt/nnm/bin/nnm -challenge
```

4. Do one of the following:
 - If you are using PVS versions 4.2.1 to 5.3.x, in your browser, navigate to <https://plugins.nessus.org/v2/offline-pvs.php>.
 - If you are using Tenable Nessus Network Monitor versions 5.4.x or later, in your browser, navigate to <https://plugins.nessus.org/v2/offline-nnm.php>.
5. Paste the challenge string from Step 3 and your Activation Code in the appropriate boxes on the web page.
6. Click **Submit**.
7. On the next page, copy the link that starts with **https://plugins.nessus.org/v2/...** and bookmark it in your browser. The other information on the page is not relevant for use with Tenable Security Center.
8. Click the bookmarked link.

The page prompts you to download a file.
9. Download the file, which is called `sc-passive.tar.gz`.



10. Save the `sc-passive.tar.gz` on the system used to access your Tenable Security Center GUI.

Note: Access the Tenable Nessus Network Monitor feed setting and change the activation from offline to Tenable Security Center.

11. Log in to Tenable Security Center as an administrator.

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.



Tenable Security Center Troubleshooting

Tenable Nessus Network Monitor server does not appear to be operational

1. Log in to Tenable Security Center as an administrator.
2. Verify that the Tenable Nessus Network Monitor server appears as **Unable to Connect** under **Status**.
3. SSH to the remote Tenable Nessus Network Monitor host to make sure the underlying operating system is operational.
4. Confirm that the Tenable Nessus Network Monitor is running (Linux example below):

```
# service nnm status

NNM is stopped
NNM Proxy (pid 3142) is running
#
```

5. If the Tenable Nessus Network Monitor service is not running, start the service:

```
# service nnm start
Starting NNM Proxy           [ OK ]
Starting NNM                 [ OK ]
#
```

Cannot add an Tenable Nessus Network Monitor server

1. Confirm that the Tenable Nessus Network Monitor proxy is listening on the same port as Tenable Security Center (port 8835 by default):

```
# ss -pan | grep 8835
tcp        0      0 0.0.0.0:8835  0.0.0.0:*    LISTEN    406/nnm
```

2. Check connectivity by telnetting from the Tenable Security Center console into the Tenable Nessus Network Monitor server on port 8835 (the Tenable Nessus Network Monitor listening port). If successful, the response includes: Escape character is '^'.



No vulnerabilities are being received from the Tenable Nessus Network Monitor server

1. Ensure that the Tenable Nessus Network Monitor service is running on the Tenable Nessus Network Monitor host.
2. Ensure that the Tenable Nessus Network Monitor appears in Tenable Security Center under **Resources > Passive Scanners** and that the status of the Tenable Nessus Network Monitor appears as **Working**.
3. Click **Edit** to ensure that the IP address or hostname, port, username, password, and selected repositories for the Tenable Nessus Network Monitor are correct.
4. Edit any incorrect entries to their correct state.
5. Click **Submit** to attempt to reinitialize the Tenable Nessus Network Monitor scanning interface.

Tenable Nessus Network Monitor 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 Security Center host allows outbound HTTPS connectivity to the Tenable Nessus Network Monitor Plugin Update Site.
3. For all other Tenable Nessus Network Monitor plugin update issues, contact Tenable Support.