Nessus Network Monitor 6.0.x User Guide

Last Updated: January 19, 2022

Table of Contents

Welcome to Nessus Network Monitor

This user guide describes the Tenable®Nessus Network Monitor®6.0.x (Patent 7,761,918 B2) architecture, installation, operation, and integration with Tenable.sc and Tenable.io, and export of data to third parties. For assistance, contact Tenable Support.

Tip: If you are new to NNM, 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. NNM also profiles traffic and detects compromised systems.

NNM 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 NNM as internet facing software.

Get Started with NNM

1. Ensure that your setup meets the minimum system requirements:
   - Hardware requirements
   - Software requirements
2. Obtain the proper license or Activation Code for NNM for your configuration.

   Note: See special activation code instructions for integration with Tenable.sc or Tenable.io.
3. Follow the installation steps for your environment:
   - Linux
   - Windows
   - macOS
   - Tenable Core
4. (Optional) Configure Virtual Switches for use with NNM.
5. Perform the initial configuration steps for NNM in the web interface.

   After configuration, NNM begins monitoring incoming traffic immediately.

   Note: If you wish to register NNM offline or run NNM in High Performance mode, you must follow several additional configuration steps.
6. Create users in NNM 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.

For more NNM deployment information, see the NNM Deployment Guide.

NNM Navigation

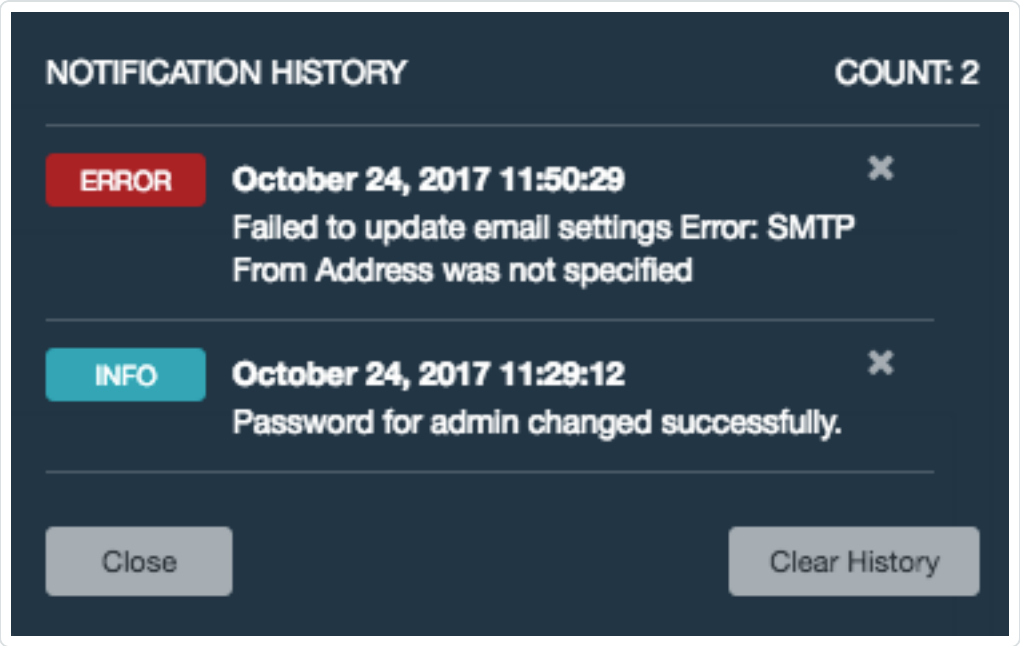
The top navigation menu displays two main pages: **Monitoring** and **Results**. All of NNM's primary analysis tasks can be performed using these two pages. Click a page name to open that page.

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 NNM.

  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 NNM 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 NNM. 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.



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 NNM Information

You can view information about your instance of NNM 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 NNM:

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

  View information for your instance of NNM.

System Requirements

This section describes the following system requirements for NNM:

- NNM Hardware Requirements
- NNM Software Requirements
- NNM Licensing Requirements

To see which versions of NNM work with Industrial Security, see IS Pairing with NNM.

NNM Hardware Requirements

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

The following chart outlines some basic hardware requirements for operating NNM:

Version	Installation scenario	RAM	Processor	Hard Disk
All Versions	NNM managing up to 50,000 hosts * (**)	2 GB RAM (4 GB RAM recommended)	2 2GHz cores	20 GB HDD minimum
	NNM managing more than 50,000 hosts **	4 GB RAM (8 GB RAM recommended)	4 2GHz cores	20 GB HDD minimum
	NNM 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 NNM.

**For optimal data collection, NNM 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: Please research your VM software vendor for comparative recommendations, as VMs typically see up to a 30% loss in efficiency compared to dedicated servers.

High Performance Mode

To run NNM 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

NNM Software Requirements

Note: Standard support for NNM 5.11 ends 01/21/2022. Tenable recommends updating to NNM 5.12 or later. Otherwise, you will not be able to report issues and bugs.

Nessus Network Monitor is available for the following platforms: