McAfee Network Security Platform 8.2
COPYRIGHT
Copyright © 2016 McAfee, Inc., 2821 Mission College Boulevard, Santa Clara, CA 95054, 1.888.847.8766, www.intelsecurity.com

TRADEMARK ATTRIBUTIONS
Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee and the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource, VirusScan are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

LICENSE INFORMATION
License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.
Contents

Preface .................................................. 7
  About this guide ..................................... 7
  Audience ............................................ 7
  Conventions ........................................ 7
  Find product documentation .................................. 8

Installing Network Security Platform

1 Network Security Platform overview .................................. 11

2 Preparation for the Manager installation .................................. 13
  Prerequisites .......................................... 13
    General settings ..................................... 13
    Other third-party applications .......................... 14
    Server requirements ................................ 14
    Manager installation with local service account privileges ....... 16
    Client requirements ................................ 16
    Java runtime engine requirements ........................ 18
    Database requirements ................................ 18
  Recommended Manager specifications .................................. 18
    Determine your database requirements ...................... 19
  Pre-installation recommendations .................................. 19
    How to plan for installation ................................ 19
    Functional requirements ................................ 20
    How to use anti-virus software with the Manager ............ 22
    User interface responsiveness ................................ 23
  Download the Manager/Central Manager executable .................... 24

3 Install the Manager/Central Manager .................................. 25
  Install the Manager ..................................... 26
  Installing the Central Manager ............................... 41
  Log files related to Manager installation and upgrade ............... 42

4 Starting the Manager/Central Manager .................................. 45
  Shut down the Manager/Central Manager services .................... 46
    Shut down the Central Manager .......................... 47
    Close all the client connections ........................ 47
    Shut down using the Network Security Platform system tray icon .... 47
    Shut down using the Control Panel ........................ 48

5 Adding a Sensor ............................................ 51
  Before you install Sensors .................................. 51
    Network topology considerations .......................... 51
    Safety measures ........................................ 52
    Usage restrictions ...................................... 53
# McAfee Network Security Platform 8.2 Installation Guide

## Unpack the Sensor

- Cable specifications
- Network Security Platform fail-closed dongle specification
- Console port pin-outs
- Auxiliary port pin-outs
- Response port pin-outs
- How to monitor port pin-outs

## Configuration of a Sensor

- Configuration overview
- Establishment of a Sensor naming scheme
- Communication between the Sensor and the Manager
- Add a Sensor to the Manager
- Configure the Sensor
- Verification of successful configuration
- How to change Sensor values
- How to add a secondary Manager IP
- Remove a secondary Manager IP

## Configuration of devices using the Manager

- Install Sensors using the wizard
- Add and configure Sensors
- Add and configure the XC Clusters
- Possible actions from the device list nodes
- Options available in the devices page
- Deploy pending changes to a device
- Update the latest software images on all devices
- Download software update files for offline devices
- Malware engine updates
- Manage failover pairs
- Specify proxy server for internet connectivity
- Configure NTP server
- Configure NTP server for a device

## Managing configuration for each device

- Configuration and management of devices
- Update configuration of a Sensor or an NTBA Appliance
- Update software for a Sensor or NTBA Appliance
- Shut down a Sensor or NTBA Appliance
- Troubleshooting your device configuration
- Upload diagnostics trace
- Management of device access
- Configure TACACS+ authentication
- Configuration of NMS objects

## Configuration of the Update Server

## Uninstallation of the Manager/Central Manager

- Uninstall using the Add/Remove program
- Uninstall using the script

## Upgrading Network Security Platform

### Overview

- Important requirements and considerations
- Migration from 1024-bit to 2048-bit encryption
- Upgrade to 2048-bit encryption
View encryption type ................................................. 123
Disable 2048-bit encryption ........................................ 126

11 Management of a heterogeneous environment 127
What are heterogeneous environments? ......................... 127
When would you need a heterogeneous environment? ......... 128
Upgrade scenarios for heterogeneous environments ........... 129
Central Manager upgrade scenarios ............................... 129
Manager upgrade scenarios ......................................... 133
Enhanced Central Manager/Manager user interface ............ 137
Feature support in a heterogeneous environment ............... 137
Heterogeneous support for NTBA devices ......................... 137
Heterogeneous environment for XC Cluster ..................... 138

12 How to upgrade the Central Manager? 139
Upgrade requirements for the Central Manager ................. 139
Upgrade path for the Central Manager and Manager ........... 139
Central Manager and Manager system requirements .......... 140
Preparation for the upgrade ........................................ 141
Review the upgrade considerations ................................ 142
Back up Network Security Platform data ........................ 142
Central Manager and operating system upgrade ............... 143
MDR Central Manager upgrade ..................................... 143
Standalone Central Manager upgrade ............................. 144
 Upgrade the signature set for the Central Manager ............ 146

13 How to Upgrade the Manager? 147
Upgrade requirements for the Manager .......................... 147
Upgrade path for the Central Manager and Manager ........... 147
Central Manager and Manager system requirements .......... 148
Preparation for the upgrade ........................................ 149
Review the upgrade considerations ................................ 149
Back up Network Security Platform data ........................ 179
Operating system upgrade scenarios ............................. 180
Manager and operating system upgrade ......................... 180
MDR Manager upgrade ............................................. 182
Standalone Manager upgrade ....................................... 183
 Resubmit Snort custom attacks for translation ................. 184
 Run additional scripts ............................................. 185

14 How to perform signature set and Sensor software upgrade 189
Difference between an update and an upgrade .................. 189
Sensor upgrade requirements ....................................... 189
Review the upgrade considerations for Sensors .............. 190
Updating Sensor software image .................................. 191
 Sensor software upgrade — Manager versus TFTP server ...... 192
 Sensor software and signature set upgrade using Manager 8.2 193
 Sensor software upgrade using a TFTP or SCP server ....... 194
 Update Sensor software in a failover pair ....................... 195

15 Upgrade information for NTBA and XC Cluster 197
Upgrade NTBA Appliance software ............................... 197
Upgrade XC Cluster ................................................. 198

16 Uninstalling the upgrade ........................................ 201
Preface

This guide provides the information you need to install your McAfee product.

Contents
  ▶ About this guide
  ▶ Find product documentation

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

Conventions

This guide uses these typographical conventions and icons.

- **Book title, term, emphasis**
  Title of a book, chapter, or topic; a new term; emphasis.

- **Bold**
  Text that is strongly emphasized.

- **User input, code, message**
  Commands and other text that the user types; a code sample; a displayed message.

- **Interface text**
  Words from the product interface like options, menus, buttons, and dialog boxes.

- **Hypertext blue**
  A link to a topic or to an external website.

  **Note:** Additional information, like an alternate method of accessing an option.

  **Tip:** Suggestions and recommendations.

  **Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data.

  **Warning:** Critical advice to prevent bodily harm when using a hardware product.
Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

Task
2. In the Knowledge Base pane, click a content source:
   - Product Documentation to find user documentation
   - Technical Articles to find KnowledgeBase articles
3. Select Do not clear my filters.
4. Enter a product, select a version, then click Search to display a list of documents.
## Installing Network Security Platform

<table>
<thead>
<tr>
<th>Chapter 1</th>
<th>Network Security Platform overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 2</td>
<td>Preparation for the Manager installation</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>Install the Manager/Central Manager</td>
</tr>
<tr>
<td>Chapter 4</td>
<td>Starting the Manager/Central Manager</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>Adding a Sensor</td>
</tr>
<tr>
<td>Chapter 6</td>
<td>Configuration of devices using the Manager</td>
</tr>
<tr>
<td>Chapter 7</td>
<td>Managing configuration for each device</td>
</tr>
<tr>
<td>Chapter 8</td>
<td>Configuration of the Update Server</td>
</tr>
<tr>
<td>Chapter 9</td>
<td>Uninstallation of the Manager/Central Manager</td>
</tr>
</tbody>
</table>
Network Security Platform overview

McAfee Network Security Platform [formerly McAfee IntruShield®] is a combination of network appliances and software built for the accurate detection and prevention of intrusions, denial of service (DoS) attacks, distributed denial of service (DDoS) attacks, malware download, and network misuse. Network Security Platform provides comprehensive network intrusion detection and can block, or prevent, attacks in real time, making it truly an intrusion prevention system (IPS).
Preparation for the Manager installation

This section describes the McAfee Network Security Manager (Manager) hardware and software requirements and pre-installation tasks you should perform prior to installing the software.

In this section, unless explicitly stated, Central Manager and Manager are commonly referred to as "Manager."

Contents
- Prerequisites
- Recommended Manager specifications
- Pre-installation recommendations
- Download the Manager/Central Manager executable

Prerequisites

The following sections list the Manager installation and functionality requirements for your operating system, database, and browser.

⚠️ We strongly recommend that you also review Network Security Platform Release Notes.

If you are installing the Manager as part of an upgrade to the latest version of Network Security Platform, also refer to Upgrading Network Security Platform on page 0.

General settings

- McAfee recommends you use a dedicated server, hardened for security, and placed on its own subnet. This server should not be used for programs like instant messaging or other non-secure Internet functions.

- You must have Administrator/root privileges on your Windows server to properly install the Manager software, as well as the installation of an embedded MySQL database for Windows Managers during Manager installation.
• It is essential that you synchronize the time on the Manager server with the current time. To keep
time from drifting, use a timeserver. If the time is changed on the Manager server, the Manager will
lose connectivity with all McAfee® Network Security Sensors (Sensors) and the McAfee® Network
Security Update Server [formerly IPS Update Server] because SSL is time sensitive.

• If Manager Disaster Recovery (MDR) is configured, ensure that the time difference between the
Primary and Secondary Managers is less than 60 seconds. (If the spread between the two exceeds
more than two minutes, communication with the Sensors will be lost.)

For more information about setting up a time server on Windows Servers, see the following
Microsoft KnowledgeBase article: http://support.microsoft.com/kb/816042/.

Once you have set your server time and installed the Manager, do not change the time on the
Manager server for any reason. Changing the time may result in errors that could lead to loss of
data.

Other third-party applications
Install a packet log viewing program to be used in conjunction with the Threat Analyzer interface. Your
packet log viewer, also known as a protocol analyzer, must support library packet capture (libpcap)
format. This viewing program must be installed on each client you intend to use to remotely log onto
the Manager to view packet logs.

Wireshark (formerly known as Ethereal) is recommended for packet log viewing. WireShark is a network
protocol analyzer for Windows servers that enables you to examine the data captured by your
Sensors. For information on downloading and using Ethereal, go to www.wireshark.com.

Server requirements
The following table lists the 8.2 Manager server requirements:

<table>
<thead>
<tr>
<th>Minimum required</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Windows Server 2012 R2 Standard Edition operating system.</td>
</tr>
<tr>
<td>Any of the following:</td>
<td></td>
</tr>
<tr>
<td>• Windows Server 2008 R2 Standard or Enterprise Edition, English operating system, SP1 (64-bit) (Full Installation)</td>
<td></td>
</tr>
<tr>
<td>• Windows Server 2008 R2 Standard or Enterprise Edition, Japanese operating system, SP1 (64-bit) (Full Installation)</td>
<td></td>
</tr>
<tr>
<td>• Windows Server 2012 R2 Standard Edition (Server with a GUI) English operating system</td>
<td></td>
</tr>
<tr>
<td>• Windows Server 2012 R2 Standard Edition (Server with a GUI) Japanese operating system</td>
<td></td>
</tr>
<tr>
<td>• Windows Server 2012 R2 Datacenter Edition (Server with a GUI) English operating system</td>
<td></td>
</tr>
<tr>
<td>• Windows Server 2012 R2 Datacenter Edition (Server with a GUI) Japanese operating system</td>
<td></td>
</tr>
<tr>
<td>Only X64 architecture is supported.</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB</td>
</tr>
<tr>
<td>CPU</td>
<td>Server model processor such as Intel Xeon</td>
</tr>
<tr>
<td>Disk space</td>
<td>100 GB</td>
</tr>
</tbody>
</table>
How to host the Manager on a VMware platform

The following are the system requirements for hosting Central Manager/Manager server on a VMware platform.

**Table 2-1  VMware ESX server requirements**

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtualization software</td>
<td>• ESXi 5.0</td>
</tr>
<tr>
<td></td>
<td>• ESXi 5.1</td>
</tr>
<tr>
<td></td>
<td>• ESXi 5.5</td>
</tr>
<tr>
<td>CPU</td>
<td>Intel Xeon® CPU ES 5335 @ 2.00 GHz; Physical Processors – 2; Logical Processors – 8; Processor Speed – 2.00 GHz</td>
</tr>
<tr>
<td>Memory</td>
<td>Physical Memory: 16 GB</td>
</tr>
<tr>
<td>Internal Disks</td>
<td>1 TB</td>
</tr>
</tbody>
</table>

**Table 2-2  Virtual machine requirements**

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Any of the following:</td>
<td>Windows Server 2012 R2 Standard Edition operating system.</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 Standard or Enterprise Edition, English operating system, SP1 (64-bit) (Full Installation)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 Standard or Enterprise Edition, Japanese operating system, SP1 (64-bit) (Full Installation)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Standard Edition (Server with a GUI) English operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Standard Edition (Server with a GUI) Japanese operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Datacenter Edition (Server with a GUI) English operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Datacenter (Server with a GUI) Japanese operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Only X64 architecture is supported.</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB</td>
<td>8 GB or more</td>
</tr>
<tr>
<td>Virtual CPUs</td>
<td>2</td>
<td>2 or more</td>
</tr>
<tr>
<td>Disk Space</td>
<td>100 GB</td>
<td>300 GB or more</td>
</tr>
</tbody>
</table>
Manager installation with local service account privileges

The Manager installs the following services as a Local Service:

- McAfee® Network Security Manager
- McAfee® Network Security Manager Database

McAfee® Network Security Manager Watchdog runs as a Local System to facilitate restart of the Manager in case of abrupt shutdown.

The Local Service account has fewer privileges on accessing directories and resources than the Local System. By default, the Manager installation directory and database directory are granted full permission to the Local Service account during installation or upgrade of Manager.

Set the permissions to a Local Service as needed in the following scenarios:

- Backup directory location: If the backup directory was different from the Manager installed directory before upgrade to the current release, full permission on these directories for a Local Service should be granted.
- Notification script execution: If a user uses a script that accesses directories or resources located in directories other than in Manager installed directories for notifications like alerts, faults etc., full permission on these directories for a Local Service should be granted.
- Database configuration: If a user has a MySQL database configured for using a directory for temporary files other than the one provided during installation, then those directories should be given full permissions for a Local Service.

Client requirements

The following are the system requirements for client systems connecting to the Manager application.

<table>
<thead>
<tr>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating system</strong></td>
<td><strong>Operating system</strong></td>
</tr>
<tr>
<td>• Windows 7, English or Japanese</td>
<td>• Windows 7, English or Japanese</td>
</tr>
<tr>
<td>• Windows 8, English or Japanese</td>
<td>• Windows 8, English or Japanese</td>
</tr>
<tr>
<td>• Windows 8.1, English or Japanese</td>
<td>• Windows 8.1, English or Japanese</td>
</tr>
</tbody>
</table>

The display language of the Manager client must be the same as that of the Manager server operating system.

<table>
<thead>
<tr>
<th><strong>RAM</strong></th>
<th>2 GB</th>
<th>4 GB</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU</strong></td>
<td>1.5 GHz processor</td>
<td>1.5 GHz or faster</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Browser</strong></th>
<th><strong>Minimum</strong></th>
<th><strong>Recommended</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Internet Explorer 9, 10, or 11</td>
<td>• Internet Explorer 11</td>
<td></td>
</tr>
<tr>
<td>• Mozilla Firefox</td>
<td>• Mozilla Firefox 20.0 or later</td>
<td></td>
</tr>
<tr>
<td>• Google Chrome (App mode in Windows 8 is not supported.)</td>
<td>• Google Chrome 24.0 or later</td>
<td></td>
</tr>
</tbody>
</table>

To avoid the certificate mismatch error and security warning, add the Manager web certificate to the trusted certificate list.
If you are using Google Chrome 42 or later, the NPAPI plug-in is disabled by default, which means that Java applet support is disabled by default. Perform the following steps to enable NPAPI plug-in:

1. In the address bar, type `chrome://flags/#enable-npapi`.
2. Click the **Enable** link in the Enable NPAPI configuration option.
3. Click **Relaunch Now** at the bottom of the page to restart Google Chrome for the changes to take effect.

For the Manager client, in addition to Windows 7, Windows 8, and Windows 8.1, you can also use the operating systems mentioned for the Manager server.

If the Manager page does not load, clear the browser cache and re-launch the browser.

The following are Central Manager and Manager client requirements when using Mac:

<table>
<thead>
<tr>
<th>Mac operating system</th>
<th>Browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Lion</td>
<td>Safari 6 or 7</td>
</tr>
<tr>
<td>• Mountain Lion</td>
<td></td>
</tr>
</tbody>
</table>

Manager client display settings (Windows)

- Access the Manager through a client browser. See **Client requirements** for the list of supported clients and browsers.
- Set your display to 32-bit color. Right-click on the Desk Top and select Screen Resolution and go to Advanced Settings | Monitor, and configure Colors to True Color (32bit).
- McAfee recommends setting your monitor’s screen area to 1440 x 900 pixels. Right-click on the Desk Top and select Screen Resolution. Set **Resolution** to 1440 x 900.
- Browsers typically should check for newer versions of stored pages. For example, Internet Explorer, by default, is set to automatically check for newer stored page versions. To check this function, open your Internet Explorer browser and go to Tools | Internet Options | General. Click the Settings button under Browsing History or Temporary Internet files, and under Check for newer versions of stored pages: select any of the four choices except for **Never**. Selecting **Never** caches Manager interface pages that require frequent updating, and not refreshing these pages might lead to system errors.
- If you are using Internet Explorer 8 or 9, then go to Tools | Compatibility View Settings and make sure Display intranet sites in Compatibility View and Display all websites in Compatibility View checkboxes are not selected.

Invoking Threat Analyzer in a Manager Client System

Note that the Manager has to be accessed using the server system's host name (https://<Manager_hostname>). The.jar file downloaded for the Threat Analyzer is signed using a certificate that is generated based on the client host name. If your client is located in a different domain than that of the Manager, you must map the host name to its IP address in your client system’s Windows hosts file.

Navigate to C:\WINDOWS\system32\drivers\etc on your client system and edit the hosts file. For example, if your host name is manager-host1, and its IP address is 102.54.94.97, your entry would appear as: 102.54.94.97 manager-host1
Internet Explorer settings when accessing the Manager from the server

McAfee recommends accessing the Central Manager and Manager from a client system. However, there might be occasions when you need to manage from the server itself. To do so, you must make the following changes to the server’s Internet Explorer options.

Regardless of whether you use a client or the server, the following Internet Explorer settings must be enabled. On Windows client operating computers, these are typically enabled by default but disabled on server operating systems.

1. In the Internet Explorer, go to Tools | Internet Options | Security | Internet | Custom Level and enable the following:
   - ActiveX controls and plug-ins: Run ActiveX controls and plug-ins.
   - ActiveX controls and plug-ins: Script ActiveX controls selected safe for scripting.
   - Downloads: File Download.
   - Miscellaneous: Allow META REFRESH.
   - Scripting: Active Scripting

2. In the Internet Explorer, go to Tools | Internet Options | Privacy and ensure that the setting is configured as something below Medium High. For example, do not set it at High or at Block all Cookies. If the setting is higher than Medium High, you receive an Unable to configure Systems. Permission denied error and the Manager configuration will not function.

Java runtime engine requirements

When you first log onto the Manager, a version of JRE is automatically installed on the client machine (if it is not already installed). This version of the JRE software is required for operation of various components within the Manager including Threat Analyzer and the Custom Attack Editor. The client JRE version bundled with the Manager is 1.7.0_72.

Database requirements

The Manager requires communication with MySQL database for the archiving and retrieval of data.

The Manager installation set includes a MySQL database for installation (that is, embedded on the target Manager server). You must use the supported operating system listed under Server requirements and must use the Network Security Platform-supplied version of MySQL (currently 5.6.20). The MySQL database must be a dedicated one that is installed on the Manager.

If you have a MySQL database previously installed on the Manager server, uninstall the previous version and install the Network Security Platform version.

See also

Server requirements on page 14

Recommended Manager specifications

McAfee® Network Security Manager (Manager) software runs on a dedicated Windows server.

The larger your deployment, the more high-end your Manager server should be. Many McAfee® Network Security Platform issues result from an under-powered Manager Server. For example, to manage 40 or more McAfee® Network Security Sensors (Sensors), we recommend larger configurations than the minimum-required specifications mentioned in Server requirements.
The Manager client is a Java web application, which provides a web-based user interface for centralized and remote Sensor management. The Manager contains Java applets. Because Java applets take advantage of the processor on the host from which they are being viewed, we also recommend that the client hosts used to manage the Network Security Platform solution exceed the minimum-required specifications mentioned in Client requirements.

You will experience better performance in your configuration and data-forensic tasks by connecting to the Manager from a browser on the client machine. Performance may be slow if you connect to the Manager using a browser on the server machine itself.

Determine your database requirements

The amount of space required for your database is governed by many factors, mostly unique to the deployment scenario. These factors determine the amount of data you want to retain in the database and the time for which the data has to be retained.

Things to consider while determining your database size requirements are:

- **Aggregate alert and packet log volume from all Sensors** — Many Sensors amount to higher alert volume and require additional storage capacity. Note that an alert is roughly 2048 bytes on average, while a packet log is approximately 1300 bytes.

- **Lifetime of alert and packet log data** — You need to consider the time before you archive or delete an alert. Maintaining your data for a long period of time (for example, one year) will require additional storage capacity to accommodate both old and new data.

As a best practice, McAfee recommends archiving and deleting old alert data regularly, and attempting to keep your active database size to about 60 GB.

For more information, see Capacity Planning, McAfee Network Security Platform Manager Administration Guide.

Pre-installation recommendations

These McAfee® Network Security Platform [formerly McAfee® IntruShield®] pre-installation recommendations are a compilation of the information gathered from individual interviews with some of the most seasoned McAfee Network Security Platform System Engineers at McAfee.

How to plan for installation

Before installation, ensure that you complete the following tasks:

- The server, on which the Manager software will be installed, should be configured and ready to be placed online.

- You must have administrator privileges for Manager server.

- This server should be dedicated, hardened for security, and placed on its own subnet. This server should not be used for programs like instant messaging or other non-secure Internet functions.

- Make sure your hardware requirements meet at least the minimum requirements.

- Ensure the proper static IP address has been assigned to the Manager server. For the Manager server, McAfee strongly recommends assigning a static IP against using DHCP for IP assignment.

- If applicable, configure name resolution for the Manager.
• Ensure that all parties have agreed to the solution design, including the location and mode of all McAfee® Network Security Sensor, the use of sub-interfaces or interface groups, and if and how the Manager will be connected to the production network.

• Get the required license file and grant number. Note that you do not require a license file for using Manager/Central Manager version 6.0.7.5 or above.

• Accumulate the required number of wires and (supported) GBICs, SFPs, or XFPs. Ensure these are approved hardware from McAfee or a supported vendor. Ensure that the required number of Network Security Platform dongles, which ship with the Sensors, are available.

• Crossover cables will be required for 10/100 or 10/100/1000 monitoring ports if they are directly connected to a firewall, router, or end node. Otherwise, standard patch cables are required for the Fast Ethernet ports.

• If applicable, identify the ports to be mirrored, and someone who has the knowledge and rights to mirror them.

• Allocate the proper static IP addresses for the Sensor. For the Sensors, you cannot assign IPs using DHCP.

• Identify hosts that may cause false positives, for example, HTTP cache servers, DNS servers, mail relays, SNMP managers, and vulnerability scanners.

See also
Server requirements on page 14

Functional requirements

Following are the functional requirements to be taken care of:

• Install Wireshark (formerly known as Ethereal http://www.wireshark.com) on the client PCs. Ethereal is a network protocol analyzer for Unix and Windows servers, used to analyze the packet logs created by Sensors.

• Ensure the correct version of JRE is installed on the client system, as described in the earlier section. This can save a lot of time during deployment.

• Manager uses port 4167 as the UDP source port to bind for IPv4 and port 4166 for IPv6. If you have Sensors behind a firewall, you need to update your firewall rules accordingly such that ports 4167 and 4166 are open for the SNMP command channel to function between those Sensors and the Manager. This applies to a local firewall running on the Manager server as well.

• Determine a way in which the Manager maintains the correct time. To keep time from drifting, for example, point the Manager server to an NTP timeserver. (If the time is changed on the Manager server, the Manager will lose connectivity with all Sensors and the McAfee® Network Security Update Server because SSL is time sensitive.)

• If Manager Disaster Recovery (MDR) is configured, ensure that the time difference between the Primary and Secondary Managers is less than 60 seconds. (If the spread between the two exceeds more than two minutes, communication with the Sensors will be lost.)

• If you are upgrading from a previous version, we recommend that you follow the instructions in the respective version's release notes or Upgrade path for the Central Manager and Manager on page 139.

Install a desktop firewall

A desktop firewall on the Manager server is recommended. Certain ports are used by the components of McAfee Network Security Platform. Some of these are required for Manager -- Sensor and Manager client-server communication. All remaining unnecessary ports should be closed.
McAfee strongly recommends that you configure a packet-filtering firewall to block connections to ports 8551, 8552, 3306, 8007, 8009, and 8552 of your Manager server. The firewall can either be a host-based or network-based. Set your firewall to deny connections to these ports if the connections are not initiated by the localhost. The only connections that should be allowed are those from the Manager server itself; that is, the localhost. For example, if another machine attempts to connect to port 8551, 8552, 3306, 8007 and 8009 the firewall should automatically block any packets sent. If you need assistance in blocking these, contact McAfee Technical Support.

Use a scanning tool such as Vulnerability Manager to ensure that there no ports open other than what is required.

If a firewall resides between the Sensor, Manager, or administrative client, which includes a local firewall on the Manager, the following ports must be opened:

<table>
<thead>
<tr>
<th>Port #</th>
<th>Protocol</th>
<th>Description</th>
<th>Direction of communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>4167 (high ports) (source port on the Manager for IPv4 communication)</td>
<td>UDP</td>
<td>Default SNMPv3 (command channel)</td>
<td>Manager--&gt;Sensor</td>
</tr>
<tr>
<td>4166 (source port on the Manager for IPv6 communication)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8500 (destination port on the Sensor)</td>
<td>UDP</td>
<td>Default SNMPv3 (command channel)</td>
<td>Manager --&gt; Sensor</td>
</tr>
<tr>
<td>8501</td>
<td>TCP</td>
<td>Proprietary (install port)</td>
<td>Sensor--&gt;Manager</td>
</tr>
<tr>
<td>8502</td>
<td>TCP</td>
<td>Proprietary (alert channel/control channel)</td>
<td>Sensor--&gt;Manager</td>
</tr>
<tr>
<td>8503</td>
<td>TCP</td>
<td>Proprietary (packet log channel)</td>
<td>Sensor--&gt;Manager</td>
</tr>
<tr>
<td>8504</td>
<td>TCP</td>
<td>Proprietary (file transfer channel)</td>
<td>Sensor--&gt;Manager</td>
</tr>
<tr>
<td>8506</td>
<td>TCP</td>
<td>Proprietary (install channel for 2048-bit certificates). For information on 2048-bit certificates, see Migration from 1024-bit to 2048-bit encryption on page 121</td>
<td>Sensor--&gt;Manager</td>
</tr>
<tr>
<td>8507</td>
<td>TCP</td>
<td>Proprietary (alert channel/control channel for 2048-bit certificates).</td>
<td>Sensor--&gt;Manager</td>
</tr>
<tr>
<td>8508</td>
<td>TCP</td>
<td>Proprietary (packet log channel for 2048-bit certificates).</td>
<td>Sensor--&gt;Manager</td>
</tr>
<tr>
<td>8509</td>
<td>TCP</td>
<td>Proprietary (Bulk file transfer channel for 2048-bit certificates).</td>
<td>Sensor--&gt;Manager</td>
</tr>
<tr>
<td>8510</td>
<td>TCP</td>
<td>Proprietary (Bulk file transfer channel for 1024-bit certificates).</td>
<td>Sensor--&gt;Manager</td>
</tr>
<tr>
<td>8555</td>
<td>TCP</td>
<td>SSL/TCP/IP (Threat Analyzer)</td>
<td>client--&gt;Manager</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>HTTPS</td>
<td>client--&gt;Manager</td>
</tr>
<tr>
<td>Port #</td>
<td>Protocol</td>
<td>Description</td>
<td>Direction of communication</td>
</tr>
<tr>
<td>--------</td>
<td>----------</td>
<td>------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>Web-based user interface</td>
<td>client--&gt;Manager (Webstart/JNLP, Console Applets)</td>
</tr>
<tr>
<td>22</td>
<td>TCP</td>
<td>SSH</td>
<td>Remote console access</td>
</tr>
</tbody>
</table>

If you choose to use non-default ports for the Install port, Alert port, and Log port, ensure that those ports are also open on the firewall.

- Note that 3306/TCP is used internally by the Manager to connect to the MySQL database.
- If you have Email Notification or SNMP Forwarding configured on the Manager, and there is firewall residing between the Manager and your SMTP or SNMP server, ensure the following ports are available as well.

### Additional communication ports

<table>
<thead>
<tr>
<th>Port #</th>
<th>Protocol</th>
<th>Description</th>
<th>Direction of communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>TCP</td>
<td>SMTP</td>
<td>Manager--&gt;SMTP server</td>
</tr>
<tr>
<td>49</td>
<td>TCP</td>
<td>TACACS+ Integration</td>
<td>Sensor--&gt;TACACS+ server</td>
</tr>
<tr>
<td>162</td>
<td>UDP</td>
<td>SNMP Forwarding</td>
<td>Manager--&gt;SNMP server</td>
</tr>
<tr>
<td>389</td>
<td>TCP</td>
<td>LDAP Integration (without SSL)</td>
<td>Manager--&gt;LDAP server</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Secure communication for MDR</td>
<td>Manager 1 --&gt;Manager 2</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Secure communication for MDR</td>
<td>Manager 2--&gt;Manager 1</td>
</tr>
<tr>
<td>514</td>
<td>UDP</td>
<td>Syslog forwarding (ACL logging)</td>
<td>Manager--&gt;Syslog server</td>
</tr>
<tr>
<td>636</td>
<td>TCP</td>
<td>LDAP Integration (with SSL)</td>
<td>Manager--&gt;LDAP server</td>
</tr>
<tr>
<td>1812</td>
<td>UDP</td>
<td>RADIUS Integration</td>
<td>Manager--&gt;RADIUS server</td>
</tr>
</tbody>
</table>

If you have McAfee ePO™ integration configured on Manager, and there is firewall between Manager and the McAfee ePO™ Server, ensure the following port is also allowed through firewall.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>8443</td>
<td>McAfee ePO™ communication port</td>
<td>Manager to McAfee ePO™ server</td>
</tr>
</tbody>
</table>

- Close all open programs, including email, the **Administrative Tools > Services** window, and instant messaging before installation to avoid port conflicts. A port conflict may prevent the application from binding to the port in question because it will already be in use.

The Manager is a standalone system and should not have other applications installed.

### How to use anti-virus software with the Manager

Some of the Manager's operations might conflict with the scanning processes of McAfee VirusScan or any other anti-virus software running on the Manager. For example, the anti-virus software might scan every temporary file created in the Manager installation directory, which might slow down the
Manager’s performance. So, be sure to exclude the Manager installation directory and its sub-directories from the anti-virus scanning processes. Specifically, be sure to exclude the following folders:

- `<Manager installation directory>\MySQL and its sub-folders. If these folders are not excluded, Network Security Platform packet captures may result in the deletion of essential MySQL files.
- `<Manager installation directory>\App\temp\tftp\in\malware\ and its sub-folders.

If you install McAfee VirusScan 8.5.0i on the Manager after the installation of the Manager software, the MySQL scanning exceptions will be created automatically, but the Network Security Platform exceptions will not.

**McAfee VirusScan and SMTP notification**

From 8.0i, VirusScan includes an option (enabled by default) to block all outbound connections over TCP port 25. This helps reduce the risk of a compromised host propagating a worm over SMTP using a homemade mail client.

VirusScan avoids blocking outbound SMTP connections from legitimate mail clients, such as Outlook and Eudora, by including the processes used by these products in an exclusion list. In other words, VirusScan ships with a list of processes it will allow to create outbound TCP port 25 connections; all other processes are denied that access.

The Manager takes advantage of the JavaMail API to send SMTP notifications. If you enable SMTP notification and also run VirusScan 8.0i or above, you must therefore add java.exe to the list of excluded processes. If you do not explicitly create the exclusion within VirusScan, you will see a Mailer Unreachable error in the Manager Operational Status to each time the Manager attempts to connect to its configured mail server.

To add the exclusion, follow these steps:

**Task**

1. Launch the VirusScan Console.
2. Right-click the task called Access Protection and choose Properties from the right-click menu.
3. Highlight the rule called Prevent mass mailing worms from sending mail.
4. Click Edit.
5. Append java.exe to the list of Processes to Exclude.
6. Click OK to save the changes.

**User interface responsiveness**

The responsiveness of the user interface, the Threat Analyzer in particular, has a lasting effect on your overall product satisfaction.

In this section we suggest some easy but essential steps, to ensure that Network Security Platform responsiveness is optimal:

- During Manager software installation, use the recommended values for memory and connection allocation.
- You will experience better performance in your configuration and data forensic tasks by connecting to the Manager from a browser on a client machine. Performance may be slow if you connect to the Manager using a browser on the server machine itself.
• Perform monthly or semi-monthly database purging and tuning. The greater the quantity of alert records stored in the database, the longer it will take the user interface to parse through those records for display in the Threat Analyzer. The default Network Security Platform settings err on the side of caution and leave alerts (and their packet logs) in the database until the user explicitly decides to remove them. However, most users can safely remove alerts after 30 days.

It is imperative that you tune the MySQL database after each purge operation. Otherwise, the purge process will fragment the database, which can lead to significant performance degradation.

• Defragment the disks on the Manager on a routine basis, with the exception of the MySQL directory. The more often you run your defragmenter, the quicker the process will be. Consider defragmenting the disks at least once a month.

Do NOT attempt to defragment the MySQL directory using the operating system’s defrag utility. Any fragmentation issues in the tables are rectified when you tune the database. For more information on database tuning, see the Manager Administration Guide.

• Limit the quantity of alerts to view when launching the Threat Analyzer. This will reduce the total quantity of records the user interface must parse and therefore potentially result in a faster initial response on startup.

• When scheduling certain Manager actions (backups, file maintenance, archivals, database tuning), set a time for each that is unique and is a minimum of an hour after/before other scheduled actions. Do not run scheduled actions concurrently.

Download the Manager/Central Manager executable

You need to download the version of the Manager or Central Manager that you want to install. You need to download it from the McAfee Update Server.

Task

1. Keep the following information handy before you begin the installation process. You must have received the following from McAfee via email.
   - Grant Number and Password – If you have not received your credentials, contact McAfee Technical Support [http://mysupport.mcafee.com/]

2. Close all open applications.

3. Go to McAfee Update Server [https://menshen.intruvert.com/] and log on, using the Grant Number and Password.

4. Go to Manager Software Updates | <required version number> folder and select the required Manager software version.

5. Download the zip and extract the setup file.
Install the Manager/Central Manager

Before you begin
Close all open programs, including email, the Administrative Tools | Services window, and instant messaging to avoid port conflicts. A port conflict may cause the Manager program to incur a BIND error on startup, hence failing initialization.

Close any open browsers and restart your server after installation is complete. Open browsers may be caching old class files and cause conflicts.

IIS (Internet Information Server) and PWS (Personal Web Server) must be disabled or uninstalled from the target server.

This section contains installation instructions for the Central Manager and Manager software on your Windows server, including the installation of a MySQL database.

In this section, unless explicitly stated, Central Manager and Manager are commonly referred to as "Manager."

Task
1 Prepare your target server for Manager software installation. See Preparing for the Manager installation.

2 Install the Manager software. See Installing the Manager.

3 Start the Manager program. During initial client login from the Manager server or a client machine, the required Java runtime engine software must be present for proper program functionality. See Starting the Manager/Central Manager.

Tasks
• Install the Manager on page 26

See also
Starting the Manager/Central Manager on page 3

Contents
• Install the Manager
• Installing the Central Manager
• Log files related to Manager installation and upgrade
Install the Manager

The steps presented are for installation of the Manager/ Central Manager software. The installation procedure prompts you to submit program and icon locations, including the location and access information of your database. Read each step carefully before proceeding to the next step.

Notes:

• Ensure that the prerequisites have been met and your target server has been prepared before commencing installation.

• You can exit the setup program by clicking Cancel in the setup wizard. Upon cancellation, all temporary setup files are removed, restoring your server to its same state prior to installation.

• After you complete a step, click Next; click Previous to go one step back in the installation process.

• Unless specified during installation, Network Security Manager is installed by default.

• The Installation Wizard creates the default folders based on the Manager Type you are installing. For example, for a first-time installation of Network Security Manager, the default location is C:\Program Files\McAfee\Network Security Manager\App. For Network Security Central Manager, it is C:\Program Files\McAfee\Network Security Central Manager\App. Similarly, the Wizard creates default folders for the MySQL database as well. For the sake of explanation, this section mentions only the folder paths for Network Security Manager unless it is necessary to mention the path for Network Security Central Manager.

• Before you begin to install, make sure the Windows Regional and Language Options are configured accordingly. For example, if you are installing it on Windows Server 2008 R2 Standard or Enterprise Edition, Japanese Operating System, SP1 (64 bit) (Full Installation), ensure that the Windows Regional and Language Options are configured for Japanese.

• When you install the Manager for the first time, it is automatically integrated with McAfee Global Threat Intelligence to send your alert, general setup, and feature usage data to McAfee for optimized protection. If you do not wish to send these data, then disable the integration with Global Threat Intelligence. However, note that to be able to query McAfee GTI IP Reputation for information on the source or target host of an attack, you need to send at least your alert data summary to McAfee. For details, see McAfee Network Security Platform Integration Guide.

• If you plan to create a new installation of the Manager in a system that currently has the Manager installed, follow these steps:
  1. Uninstall the Manager.
  2. Go to the installation directory.
  3. Delete all the previous Manager default folders.
  4. Once the folders are removed restart the system then continue with the Manager installation.
**Task**

1. Log on to your Windows server as *Administrator* and close all open programs.

2. Run the Manager executable file that you downloaded from the McAfee Update Server. The Installation Wizard starts with an introduction screen. See also the Manager/Central Manager executable.

   ![Manager Installation Wizard](image-url)
3 Confirm your acknowledgement of the License Agreement by selecting I accept the terms of the License Agreement.
4 From the Manager Type drop-down list, select Network Security Manager or Network Security Central Manager. For an upgrade, Network Security Manager or Network Security Central Manager is displayed accordingly, which you cannot change.

Once installed, the Network Security Central Manager cannot be converted to Network Security Manager or vice versa.

5 Choose a folder where you want to install the Manager software.
For a first-time installation, the default location is C:\Program Files\McAfee\Network Security Manager\App. For an upgrade, it is the same location as that of the earlier version.

- **Restore Default Folder**: Resets the installation folder to the default location.
- **Choose**: Browse to a different location.

**⚠️** Installing the Manager software on a network-mapped drive may result in improper installation.

**ℹ️** The Manager software cannot be installed to a directory path containing special characters such as a comma (,), equal sign (=), or pound sign (#).

6 Choose a location for the Manager shortcut icon:
- **On the Start Menu**
- **On the Desktop**
- **On the Quick Launch Bar**
- **Create Icons for All Users**

You can include or remove multiple options by selecting the relevant checkboxes.
7 Type the password for your default user.

Use a combination of alphabets [both uppercase (A-Z) and lowercase (a-z)], numbers [0-9] and/or, special characters like "~ ` ! @ # $ % - * _ + [ ] : ; , ( ) ? { }".

Do not use null or empty characters.
8 Set the following:

- **Database Type** is displayed as MySQL.
  You must use only the MySQL bundled with the Manager installation file. Provide the database connection information as follows:

- **Database Name**: Type a name for your database. It is recommended you keep the default entry of if intact.
  The MySQL database name can be a combination of alphabets [both uppercase (A-Z) and lowercase (a-z)], numbers [0-9] and/or, special characters like dollar and underscore [$_].

- **Database User**: Type a user name for database-Manager communication; this account name is used by the Manager. This account enables communication between the database and the Manager.
  When typing a user name, observe the following rules:
  - The MySQL database user name can be a combination of alphabets [both uppercase (A-Z) and lowercase (a-z)], numbers [0-9] and/or, special characters like "~`!@#$%^*-_[]':;", ( ) ? { }".
  - The first character must be a letter.
  - Do not use null or empty characters.
  - Do not use more than 16 characters.

- **Database Password**: Type a password for the database-Manager communication account. This password relates to the **Database User** account.
  - The MySQL database password can be a combination of alphabets [both uppercase (A-Z) and lowercase (a-z)], numbers [0-9] and/or, special characters like "~`!@#$%^*-_[]':;", ( ) ? { }".
  - Do not use null or empty characters.

  ![Warning] This password is not the root password for database management; you will set the root password in a subsequent step.

- **MySQL Installation Directory**: Type or browse to the absolute location of your selected Manager database. For a first-time installation, the default location is: C:\Program Files\McAfee\Network Security Manager\MySQL. For upgrades, the default location is the previous installation directory. You can type or browse to a location different from the default. However, the database must be on the same server as the Manager.
9 Click Next.

If you are creating a new database, Network Security Platform a message appears asking to confirm that you really want to create a new database. Click Continue to continue with the installation.
10 Type the root password for your database. If this is the initial installation, type a root password and then type it again to confirm.

The **MySQL Root Password** is required for root access configuration privileges for your MySQL database. Use a combination of alphabets [both uppercase (A-Z) and lowercase (a-z)], numbers [0-9] and/or, special characters like "~ ! @ $ % - * _ + [ ] : ; , ( ) ? { }".

Do not use null or empty characters.

For security reasons, you can set a **MySQL Root Password** that is different from the **Database Password** that you set in a previous step.

11 Choose the folder in which you wish to install the Solr database.

The Manager uses Apache Solr for quick retrieval of data. Solr is an open-source search platform from the Apache Lucene project. The Manager makes use of Solr to retrieve data to be displayed in the Manager Dashboard and Analysis tabs.

For a first-time installation, the default location is `C:\Program Files\McAfee\Network Security Manager\Solr`.

The following options are available in the wizard:

- **Restore Default Folder**: Resets the installation folder to the default location.
- **Choose**: Click to browse to a different location.
Solr is used by the Manager to enhance database access. This helps in faster data refresh in the Manager dashboard and monitors.

Verify that you have at least 20 GB of free space before you install Solr.

The Solr installation directory screen will not be displayed during the Network Security Central Manager installation.
12 Click Next.

The 8.2 Manager installation is supported only on 64-bit OS. If you try installing in a 32-bit OS a warning message will be displayed. Click Ok on the warning message to exit the Manager installation wizard.

Enter a value to set Actual Maximum RAM Usage.

The RAM size indicated here determines the recommended amount of program memory (virtual memory) to allocate for server processes required by Network Security Platform. Since Jboss memory uses hard-disk-based memory (program memory), the total amount of both can exceed the Manager server’s RAM memory size.

The Recommended Maximum RAM Usage is Physical Server Memory divided by 2 or 1170 MB - whichever is greater. The Actual Maximum RAM Usage can be between 768 MB and three-fourth of the Physical Server Memory size.
13 Set the following (applicable only Network Security Manager):

- **Number of Sensors**: Select the numbers of McAfee® Network Security Sensors (Sensors) to be managed by this installation of the Manager.

- **Actual Maximum DB connections**: Enter the maximum number of concurrent database connections allowed from the Manager. The default is 40. The recommended number indicated above is based on the **Number of Sensors**.

14 If the Manager server has multiple IPv4 or IPv6 addresses, you can specify a dedicated address that it should use to communicate with the Network Security Platform devices.
To specify an IP address, select **Use IPV4 Interface?** or **Use IPV6 Interface?** and then select the address from the corresponding drop-down list.

In the Wizard, the option to specify a dedicated interface is displayed only if the Manager has more than one IPv4 or IPv6.

- When configuring the sensors, you need to configure the same IP that you selected here as the IP address used to communicate with the Network Security Platform devices.

- If the Manager has an IPv6 address, then you can add Sensors with IPv6 addresses to it.
- If an IP address is not displayed in the drop-down list or if a deleted IP address is displayed, then cancel the installation, restart the server, and re-install the Manager.
- Post-installation, if you want to change the dedicated IP address that you already specified, you need to re-install the Manager.

15 In the **Manager Installation wizard**, review the **Pre-Installation Summary** section for accurate folder locations and disk space requirements. This page lists the following information:

- **Product Name**: Shows product as Manager (for both Manager and Central Manager).
- **Install Folder**: The folder you specified in Step 5.
- **Shortcut Folder**: The folder you specified in Step 6.
- **Manager type**: Type of Manager being installed.
- **Database**: The type of database being used by Network Security Platform, which is MySQL.
- **Database Installation location**: The location on your hard drive where the database is to be located, which you specified in Step 7.

- **Dedicated Interface**: The IPv4 and IPv6 addresses that you specified for Manager-to-Sensor communication are displayed.
16 Click Install.

The Manager software and the MySQL database are installed to your target server. In case of an upgrade, database information is synchronized during this process.

Post-installation, you can check the initdb.log (from <Manager install directory>\App) for any installation errors. In case of errors, contact McAfee Support with initdb.log.

17 A congratulatory message appears upon successful installation.

The Manager Installation Wizard displays the following fields.

- URL for access web-based user interface. For example, if the Manager server's computer name is Callisto, then the url is https://Callisto

  - Default username

  - Launch the Web-based user interface on exit? checkbox

(by default, the check box is selected).
18 Click Done.

If the installation wizard prompts for a restart, it is recommended to restart the system before logging onto the Manager.

The restart option might be displayed if there are any pending OS flags reset required by the installer, for proper removal/updates of temporary files used during installation.

19 Use the shortcut icon that you created to begin using the Manager.

The Manager program opens by default in HTTPS mode for secure communication.

All the Manager services will be started after clicking the Done button at the end of installation.

20 Type a valid login ID (default: admin) and password (default: admin123) for Network Security Manager and login ID (default: nscmadmin) and password (default: admin123) for Network Security Central Manager.

Upon initial client logon, you are required to install Java applications. See Java installation for client systems.

21 You can use the Manager Initialization Wizard to complete the basic configuration steps.

See also
Prerequisites on page 13
Download the Manager/Central Manager executable on page 24

Installing the Central Manager

The installation of the Central Manager is similar to that of Manager. Follow the steps provided in Installing the Manager.
During installation, you need to select the Manager type as Network Security Central Manager. By default, Network Security Manager is selected.

Figure 3-1 Central Manager installation

Sensor communication Interface is not present during Central Manager installation.

There can be only one active installation on a Windows machine. Every Central Manager and Manager installation has its own MySQL database. No centralized database exists in an Central Manager setup.

Central Manager has to be of equal or later version than the corresponding Managers.

See also
Install the Manager on page 26

Log files related to Manager installation and upgrade

Two log files specifically related to Manager/Central Manager installation and upgrade are available:

- **mgrVersion.properties**: Every fresh installation or upgrade of the Central Manager or Manager is logged to this file. Each entry contains the version of the Central Manager or Manager that you installed or upgraded to. It also contains the date and time of when you performed this action. This can help you troubleshoot issues. For example, you can go through this log to correlate an issue with a specific Manager upgrade. This file is stored at `<Central Manager or Manager install directory>\App\config`.

- **dbconsistency.log**: When you upgrade the Central Manager or Manager, the installed database schema is compared against the actual schema of the version you are upgrading to. This comparison is to check for any inconsistencies. The details of this comparison are logged to this file as error, warning, and informational messages. This file is stored at `<Central Manager or Manager install directory>\App`. You can verify this log to check if any database inconsistency is the cause of an issue. This file is updated whenever you upgrade the Central Manager or Manager.
Warning message during downgrade

Downgrade of Central Manager or Manager is not supported. To revert to an earlier version, you must uninstall your current version, install the older version, and restore the database backup from that older version. There can be instances when you may inadvertently attempt to install an older version of the Central Manager or Manager when a later version is already installed. In such cases, the Installation Wizard displays the following warning message.

![Figure 3-2 Attempted Download Detected dialog](image)

**Figure 3-2 Attempted Download Detected dialog**
Install the Manager/Central Manager
Log files related to Manager installation and upgrade
Starting the Manager/Central Manager

This section assumes you have permissions granting you access to the software. In Network Security Platform, this translates to a Super User role at the root admin domain. Your actual view of the interface may differ, depending on the role you have been assigned within Network Security Platform. For example, certain tasks may be unavailable to you if your role denies you access. If you find you are unable to access a screen or perform a particular task, consult your Network Security Platform Super User.

For testing purposes, you can access the Manager from the server. For working with the Manager/Central Manager, McAfee recommends that you access the server from a client machine. Running the Manager/Central Manager interface client session on the server can result in slower performance due to program dependencies, such as Java, which may consume a lot of memory.

To view the Manager/Central Manager interface, do the following:

**Task**

1. Make sure the following services are running on the Manager server:
   - McAfeeNetwork Security Manager
   - McAfeeNetwork Security Manager Database
   - McAfee Network Security Manager Watchdog. The default Windows Startup Type for this service is manual. So, you might have to manually start this service.

   See Manager installation with Local Service account privileges section.

   If you have installed the Central Manager, then make sure the following services are running on the Central Manager server:
   - McAfee Network Security Central Manager
   - McAfee Network Security Central Manager Database
   - McAfee Network Security Central Manager Watchdog. The default Windows Startup Type for this service is manual. So, you might have to manually start this service.

   Start the services using one of these methods to start the Manager, Database, and Watchdog services:
   - Select Start | Settings | Control Panel. Double-click Administrative Tools, and then double-click Services. Locate the services starting with McAfee Network Security Manager.
   - Right-click on the Manager icon at the bottom-right corner of your server and start the required service. The database service is not available with this option.
2 Open the Manager
- Server - Double-click the shortcut icon that you created during installation.
- Client machine -
  Start your browser (Internet Explorer 8.0 9.0 or 10, or Firefox 7.0) and then type the URL of the Manager server:
  https://<hostname or host-IP>

3 Log on to the Manager by entering the default logon ID and password.

   If pop-up blocker settings is enabled in the browser, you will not be able to type your login credentials. In such an instance, disable the pop-up blocker settings in your browser and then try to access the Manager using your login ID and password. If the pop-up blocker is enabled, the login and password text boxes are disabled and it remains disabled till you disable the pop-up blocker and refresh the browser.

The Manager software requires Java runtime engine software for some of its components. When you first log onto the Manager from a client system, you are prompted to download and install the appropriate version of the JRE software.

You must download and install these programs for proper functioning of the Manager program. See Java runtime engine requirements.

Tasks
- Shut down the Manager/Central Manager services on page 46

## Shut down the Manager/Central Manager services

A proper shutdown of the Manager/Central Manager prevents data corruption by allowing data transfer and other processes to gracefully end prior to machine shutdown.

**Shutting down the Manager**

A proper shutdown of the Manager services requires the following steps be performed:

**Task**

1 Close all client connections. See Closing all client connections.
2 Stop the McAfee® Network Security Manager service.
3 Stop the McAfee® Network Security Manager Watchdog service.
4 Stop the McAfee® Network Security Manager MySQL service.

**Tasks**

- Shut down the Central Manager on page 47
- Close all the client connections on page 47
- Shut down using the Network Security Platform system tray icon on page 47
- Shut down using the Control Panel on page 48

**See also**

Close all the client connections on page 47
Shut down the Central Manager

Task
1. Close all client connections.
2. Stop the McAfee® Network Security Central Manager service.
3. Stop the McAfee® Network Security Central Manager Watchdog service.
4. Stop the McAfee® Network Security Central Manager MySQL service.

In a crash situation, the Manager/Central Manager will attempt to forcibly shut down all its services.

Close all the client connections
The following procedure details the recommended steps for determining which users are currently logged on to the Manager/Central Manager server. All client-session configuration and data review should be gracefully closed prior to server shutdown.

Task
1. Log onto the Manager/Central Manager server through a browser session.
2. In the Dashboard, view the Manager Summary to view the currently logged on users.
3. Ask the users to close all Manager windows such as Threat Analyzer and Manager Home page and log out of all open browser sessions.

Shut down using the Network Security Platform system tray icon

Task
1. Right-click the Manager/Central Manager icon in your System Tray. The icon displays as an "M" enclosed within a shield.

Figure 4-1 Network Security Manager Service

2. Select Stop Manager or Stop Central Manager. Once this service is completely stopped, continue to the next step.

Figure 4-2 Stop Central Manager Service option

3. Go to Start | Settings | Control Panel.
4. Open **Administrative Tools**.

5. Open **Services**.

6. Find and select **McAfee® Network Security Manager Database** or **McAfee® Network Security Central Manager Database** in the services list under the "Name" column.

7. Click the **Stop Service** button. Once this service is completely stopped, continue to the next step.

8. You can now safely shut down/reboot your server.

**Shut down using the Control Panel**

**Task**

1. Go to **Start | Settings | Control Panel**.

2. Open **Administrative Tools**.

3. Open **Services**.

4. Select **Network Security Manager Service** or **Network Security Central Manager Service** in the services list under the **Name** column.
5 Click the **Stop Service** button.

Once this service is completely stopped, continue to the next step.

---

6 Find and select McAfee Network Security Manager Database or McAfee Network Security Central Manager Database in the services list under the "Name" column.

7 Click the **Stop Service** button. Once this service is completely stopped, continue to the next step.

8 You can now safely shut down/reboot your server.
Starting the Manager/Central Manager
Shut down the Manager/Central Manager services
Adding a Sensor

After installing the Manager software and a successful logon session, the next step is to add one or more Sensors to the Manager. For more information on configuring a Sensor, see McAfee Network Security Platform CLI Reference Guide and McAfee Network Security Platform IPS Administration Guide.

For information on adding and deploying a Virtual IPS Sensor, see Virtual IPS Sensor deployment, Network Security Platform IPS Administration Guide.

Contents
- Before you install Sensors
- Cable specifications
- Configuration of a Sensor

Before you install Sensors

This section describes best practices for deployment of McAfee Network Security Sensor (Sensor) on your network and is generic to all Sensor appliance models.

Topics include system requirements, site planning, safety considerations for handling the Sensor, and usage restrictions that apply to all Sensor models.

Sensor specifications, such as physical dimensions, power requirements, and so on are described in each Sensor model's Product Guide.

Network topology considerations

Deployment of McAfee® Network Security Platform [formerly McAfee® IntruShield®] requires basic knowledge of your network to help determine the level of configuration and amount of installed Sensors and McAfee Network Security Manager (Manager) required to protect your system.

The Sensor is purpose-built for the monitoring of traffic across one or more network segments.
**Safety measures**

Please read the following warnings before you install the product. Failure to observe these safety warnings could result in serious physical injury.

- Read the installation instructions before you connect the system to its power source.
- To remove all power from the Sensor, unplug all power cords, including the redundant power cord.
- Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
- The Sensor has no ON/OFF switch. Plug the Sensor into a power supply ONLY after you have completed rack installation.
- Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.
- This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.
- Do not remove the outer shell of the Sensor. Doing so will invalidate your warranty.
- Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Blank faceplates and cover panels prevent exposure to hazardous voltages and currents inside the chassis, contain electromagnetic interference (EMI) that might disrupt other equipment, and direct the flow of cooling air through the chassis.
- To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

**Fiber-optic ports**

- Fiber-optic ports (for example, FDDI, OC-3, OC-12, OC-48, ATM, GBIC, and 100BaseFX) are considered Class 1 laser or Class 1 LED ports.

- These products have been tested and found to comply with Class 1 limits of IEC 60825-1, IEC 60825-2, EN 60825-1, EN 60825-2, and 21CFR1040.

- To avoid exposure to radiation, do not stare into the aperture of a fiber-optic port. Invisible radiation might be emitted from the aperture of the port when no fiber cable is connected.
Usage restrictions
The following restrictions apply to the use and operation of a Sensor:

- You may not remove the outer shell of the Sensor. Doing so will invalidate your warranty.
- The Sensor appliance is not a general purpose workstation.
- McAfee prohibits the use of the Sensor appliance for anything other than operating the Network Security Platform.
- McAfee prohibits the modification or installation of any hardware or software in the Sensor appliance that is not part of the normal operation of the Network Security Platform.

Unpack the Sensor
To unpack the Sensor:

Task
1. Place the Sensor box as close to the installation site as possible.
2. Position the box with the text upright.
3. Open the top flaps of the box.
4. Remove the accessory box.
5. Verify you have received all parts. These parts are listed on the packing list and in Contents of the Sensor box, below.
6. Pull out the packing material surrounding the Sensor.
7. Remove the Sensor from the anti-static bag.
8. Save the box and packing materials for later use in case you need to move or ship the Sensor.

See also
Contents of the Sensor box on page 53

Contents of the Sensor box
The following accessories are shipped in the Sensor box:

- One Sensor
- One power cord. McAfee provides a standard, 2m NEMA 5-15p (US) power cable (3 wire). International customers must procure a country-appropriate power cable with specific v/a ratings.
- One set of rack mounting ears.
- Fail-closed dongles (two for the I-1200, four for the I-1400, six for I-2700).
- One printed McAfee Network Security Platform Quick Start Guide.
- Release notes.

Cable specifications
This section lists the specifications for all cables to use with McAfee Network Security Sensor (Sensor).
Network Security Platform fail-closed dongle specification

The I-1200 and I-1400 Sensors, for example, require the dongle specified in the following for all monitoring modes requiring a fail-closed connection. Configurations requiring the dongle are described in the corresponding McAfee Network Security Platform Sensor Product Guide chapter on cabling the Sensor.

![Fail-closed dongle specification](image)

Figure 5-1  Fail-closed dongle specification

Console port pin-outs

McAfee supplies a console cable. The specifications for this cable are as follows:

The Console port is pinned as a DCE so that it can be connected to a PC's COM1 port with a straight-through cable.

<table>
<thead>
<tr>
<th>Pin #</th>
<th>Signal</th>
<th>Direction on Sensor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DCD</td>
<td>Output</td>
</tr>
<tr>
<td>2</td>
<td>RXD</td>
<td>Output</td>
</tr>
<tr>
<td>3</td>
<td>TXD</td>
<td>Input</td>
</tr>
<tr>
<td>4</td>
<td>DTR</td>
<td>Input</td>
</tr>
<tr>
<td>5</td>
<td>GND</td>
<td>not applicable</td>
</tr>
<tr>
<td>6</td>
<td>DSR</td>
<td>Output</td>
</tr>
<tr>
<td>7</td>
<td>RTS</td>
<td>Input</td>
</tr>
<tr>
<td>8</td>
<td>CTS</td>
<td>Output</td>
</tr>
<tr>
<td>9</td>
<td>No Connection</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

Auxiliary port pin-outs

The Auxiliary (Aux) port is pinned as a DTE so that it can be connected to a modem with a straight-through cable.

<table>
<thead>
<tr>
<th>Pin #</th>
<th>Signal</th>
<th>Direction on Sensor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DCD</td>
<td>Input</td>
</tr>
<tr>
<td>2</td>
<td>RXD</td>
<td>Input</td>
</tr>
</tbody>
</table>
### Management port pin-outs

The Management (Mgmt) port uses a Cat 5/Cat 5e cable.

<table>
<thead>
<tr>
<th>Pin #</th>
<th>Signal</th>
<th>Direction on Sensor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TxD+</td>
<td>Output</td>
</tr>
<tr>
<td>2</td>
<td>TxD-</td>
<td>Output</td>
</tr>
<tr>
<td>3</td>
<td>RxD+</td>
<td>Input</td>
</tr>
<tr>
<td>4</td>
<td>These pins are terminated to ground through a 75 ohm resistor &amp; capacitor.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>RxD-</td>
<td>Input</td>
</tr>
<tr>
<td>7</td>
<td>These pins are terminated to ground through a 75 ohm resistor &amp; capacitor.</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Category 5 Enhanced (Cat 5e) cable is required for transmission speeds up to 1 Gigabit per second (Gigabit Ethernet). For Ethernet networks running at 10 or 100 Mbps, Category 5 (Cat 5) OR Cat 5e cable can be used.

Throughout this guide, cabling specifications will be mentioned as Cat 5/Cat 5e.

### Response port pin-outs

The Response ports use Cat 5/Cat 5e cables.

<table>
<thead>
<tr>
<th>Pin #</th>
<th>Signal</th>
<th>Direction on Sensor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TxD+</td>
<td>Output</td>
</tr>
<tr>
<td>2</td>
<td>TxD-</td>
<td>Output</td>
</tr>
<tr>
<td>3</td>
<td>RxD+</td>
<td>Input</td>
</tr>
<tr>
<td>4</td>
<td>These pins are terminated to ground through a 75 ohm resistor &amp; capacitor.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>RxD-</td>
<td>Input</td>
</tr>
<tr>
<td>7</td>
<td>These pins are terminated to ground through a 75 ohm resistor &amp; capacitor.</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How to monitor port pin-outs

The following ports are relevant for monitoring port pin-outs.

- Gigabit Ethernet (GE) ports
- Fast Ethernet (FE) 10/100/1000 ports

See also

Gigabit Ethernet (GE) ports on page 56
Fast Ethernet (FE) 10/100/1000 ports on page 56

Gigabit Ethernet (GE) ports

GBIC monitoring ports use cables appropriate for the type of GBIC you choose to use. This includes cabling for failover between the GBIC ports on two failover Sensors.

Fast Ethernet (FE) 10/100/1000 ports

10/100/1000 monitoring ports use Cat 5/Cat 5e cables. The Sensor’s normal mode of operation, using pins 1&2 and 3&6, is to fail-open—that is, data will continue to pass through the Sensor allowing continued data flow. In this mode, pins 4&5 are terminated to ground via 75 ohm and a capacitor.

<table>
<thead>
<tr>
<th>Pin #</th>
<th>Signal</th>
<th>Direction on Sensor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TxD+ FO</td>
<td>(See text above.)</td>
</tr>
<tr>
<td>2</td>
<td>TxD- FO</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>RxD+</td>
<td>Input</td>
</tr>
<tr>
<td>4</td>
<td>TxD+ FC</td>
<td>Reserved for use in the fail-closed dongle.</td>
</tr>
<tr>
<td>5</td>
<td>TxD- FC</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>RxD-</td>
<td>Input</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>These pins are terminated to ground through a 75 ohm resistor &amp; capacitor.</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Configuration of a Sensor

This section describes how to configure a McAfee Network Security Sensor (Sensor). This information is generic to all Sensor appliance models.

The information presented in this chapter was developed based on devices in a specific lab environment. All Sensors used in this document started with a cleared (default) configuration. If you are working in a live network, please ensure that you understand the potential impact of any command before using it. For more information on the available Sensor CLI commands, see the McAfee Network Security Platform CLI Guide.

Configuration overview

At a high level, the process of configuring the Sensor involves the following steps. Detailed instructions follow in subsequent sections of this chapter.

Task

1. (Pre-installation) Establish a Sensor naming scheme for your Sensors.

2. Install and bring up the Sensor. (This information is described in detail in the Product Guide for each Sensor model.)
3 Add the Sensor to Manager using the McAfee Network Security Manager (Manager) Configuration page.

4 Configuring the Sensor with a unique name and shared key value.

5 Configuring the Sensor's network information (for example, IP address and netmask, Sensor name, and so on).

6 Verify that the Sensor is on the network. (See Configuring the Sensor)

7 Verify connectivity between the Manager and the Sensor. (See Verifying successful configuration)

See also

Establishment of a Sensor naming scheme on page 57
Add a Sensor to the Manager on page 57
Configure the Sensor on page 58
Verification of successful configuration on page 61

Establishment of a Sensor naming scheme

Once you have configured a Sensor with a name, you will be unable to change the name without reconfiguring the Sensor. McAfee recommends that you establish an easily recognizable naming scheme prior to deployment that indicates your Sensors' locations or purposes, and which ensures unique names. The Manager will not recognize two Sensors with identical names.

Sensors are represented by name in several areas of McAfee Network Security Platform and its alert data: the Manager Configuration page, alert and configuration reports, and the Threat Analyzer. Thus, it is a good idea to make your Sensor naming scheme clear enough to interpret by anyone who might need to work with the system or its data.

For example, if you were deploying Sensors at a university, you might name your Sensors according to their location on the campus: Sensor1_WeanHall, Sensor2_WeanHall, Sensor1_StudentUnion, Sensor1_Library, and so on.

The Sensor name is a case-sensitive alphanumeric character string up to 25 characters. The string can include hyphens, underscores, and periods, and must begin with a letter.

Communication between the Sensor and the Manager

The Sensor initiates all communication with the Manager server until secure communication is established between the them. Later, configuration information is pushed from Manager to Sensor. The Manager does not poll the network to discover the Sensor.

All communication between the Manager and Sensor is secure. Refer to KnowledgeBase article KB55587 for details.

Add a Sensor to the Manager

After a Sensor is configured with a name and shared key value, you can add the Sensor in the Manager Configuration page.

Adding a physically installed and network-connected Sensor to the Manager activates communication between them.

The process of installing and connecting a Sensor is described in the McAfee Network Security Platform Product Guide for each Sensor model.
The following steps describe how to add a Sensor to the Manager:

**Task**

1. Start the Manager software.
2. Log on to the Manager (the default username is admin; the default password is admin123).
3. In the System page, select the Domain to which you want to add the Sensor and then select Global | Add and Remove Devices | New.

   The Add New Device form appears.

   ![Add New Device window](image)

   **Figure 5-2 Add New Device window**

4. Type the same Device Name you entered on the Sensor.

   The exact same Sensor Name and Shared Secret must also be entered into the CLI of the Sensor during physical installation. If not, the Manager will not recognize a Sensor trying to communicate with the Manager.

5. Ensure the selected Sensor type is IPS Sensor

6. Enter the Shared Secret.

7. Confirm the Shared Secret.

8. Select an Updating Mode as Online or Offline.

   Online is the default mode.

9. (Optional) Type the Contact Information and Location.

10. Click Save or click Cancel to end the installation.

**Configure the Sensor**

At any time during configuration, you can type ? to get help on the Sensor CLI commands. To see a list of all commands, type commands. These commands are described in the McAfee Network Security Platform CLI Guide.

! The first time you configure a Sensor, you must have physical access to the Sensor.

If you are moving a Sensor to a new environment and wish to wipe the Sensor back to its factory default settings, start by typing factorydefaults from the CLI. See the McAfee Network Security Platform CLI Guide for specific details on the usage of command.
Task

1 Open a hyperterminal session to configure the Sensor. (For instructions on connecting to the Console port, see the section Cabling the Console Port, in the McAfee Network Security Platform Product Guide for your Sensor model.)

2 At the login prompt, log on to the Sensor using the default username
   admin and password admin123.

   McAfee strongly recommends that you change the default password later for security purposes as described in Step 9.

   By default, the user is prompted for configuration set up, immediately after login. Else, the user can choose to start the setup later from command prompt using the setup command. For more information, see the McAfee Network Security Platform CLI Guide.

3 Set the name of the Sensor. At the prompt, type:

   set sensor name <WORD>

   The Sensor name is a case-sensitive alphanumeric character string up to 25 characters. The string can include hyphens, underscores, and periods, and must begin with a letter.

   For example, set Sensor name Engineering_Sensor1

4 Set the IP address and subnet mask of the Sensor. At the prompt, type:

   set sensor ip <A.B.C.D> <E.F.G.H>

   Specify a 32-bit address written as four eight-bit numbers separated by periods as in
   <A.B.C.D>

   where:
   • A,B,C or D is an eight-bit number between 0-255.
   • <E.F.G.H> represents the subnet mask.

   For example,
   set sensor ip 192.34.2.8 255.255.255.0 Or Specify an IPv6 address as given below:
   set sensor ipv6 <A:B:C:D:E:F:G:H/I>

   where:
   • A:B:C:D:E:F:G:H> is a 64-bit address written as octet (eight groups) of four hexadecimal numbers, separated by colons. Each group A,B,C,D (etc) represents a group of hexadecimal numbers between 0000-FFFF. This is followed by a prefix length I with value between 0 and 128. For example, set sensor ipv6 2001:0db8:8a2e:0000:0000:0000:0000:0111/64

   If one or more four-digit group(s) is 0000, the zeros may be omitted and replaced with two colons (::). For example, set sensor ipv6 2001:0db8:8a2e::0111/64

   Setting the IP address for the first time—that is, during the initial configuration of the Sensor—does not require a Sensor reboot. Subsequent changes to the IP address will, however, require that you reboot the Sensor for the change to take effect. If a reboot is necessary, the CLI will prompt you to do so. For information on rebooting, see Conditions requiring a Sensor reboot, McAfee Network Security Platform Troubleshooting Guide.

5 If the Sensor is not on the same network as the Manager, set the address of the default gateway
Note that you should be able to ping the gateway (that is, gateway should be reachable). At the prompt, type: `set sensor gateway <A.B.C.D>`

Use the same convention as the one for Sensor IP address. For example, `set sensor gateway 192.34.2.8`

Or specify an IPv6 address of the gateway for the Manager server as given below:

`set sensor gateway-ipv6 <A:B:C:D:E:F:G:H>`

where:

- `<A:B:C:D:E:F:G:H>` is a 128-bit address written as octet (eight groups) of four hexadecimal numbers, separated by colons. Each group A,B,C,D etc is a group of hexadecimal numbers between 0000-FFFF. For example, `set sensor gateway-ipv6 2001:0db8:8a2e::0111`

If one or more four-digit group(s) is 0000, the zeros may be omitted and replaced with two colons (::). For example, `set sensor gateway-ipv6 2001:0db8:8a2e::0111`

6 Set the IPv4 or IPv6 address of the Manager server. At the prompt, type:

`set manager ip <A.B.C.D>`

Use the same convention as the one for Sensor IP address. For example, `set manager ip 192.34.3.2`

Or type an IPv6 address of the Manager server, as given below: `set manager ip <A:B:C:D:E:F:G:H>`

where:

- `<A:B:C:D:E:F:G:H>` is a 128-bit address written as octet (eight groups) of four hexadecimal numbers, separated by colons. Each group (A,B,C,D etc) is a group of hexadecimal numbers between 0000-FFFF. For example: `set manager ip 2001:0db8:8a2e::0111`

If one or more four-digit group(s) is 0000, the zeros may be omitted and replaced with two colons (::). For example: `set manager ip 2001:0db8:8a2e::0111`

7 Ping the Manager from the Sensor to determine if your configuration settings to this point have successfully established the Sensor on the network. At the prompt, type: `ping <manager IP address>`

The success message "host <ip address> is alive " appears. If not, type `show` to verify your configuration information and check to ensure that all information is correct. If you run into any difficulties, see McAfee Network Security Platform Troubleshooting Guide.

8 Set the shared key value for the Sensor. This value is used to establish a trust relationship between the Sensor and the Manager.

At the prompt, type:

`set sensor sharedsecretkey`

The Sensor then prompts you to enter a shared secret key value. Type the shared secret key value at the prompt. The Sensor then prompts you to verify the value. Type the value again.
(Optional, but recommended) Change the Sensor password. At the prompt, type:

```
passwd
```

The Sensor prompts you to enter the new password and prompts you for the old password. A password must be between 8 and 25 characters, is case-sensitive, and can consist of any alphanumeric character or symbol.

McAfee strongly recommends that you choose a password with a combination of characters that is easy for you to remember but difficult for someone else to guess.

To exit the session, type

```
exit
```

Verification of successful configuration

There are three ways to check that the Sensor is configured and available:

- On the Sensor, type `status` (For more information on the `status` command, see the McAfee Network Security Platform CLI Guide.)
- In the Manager Dashboard, check the System Health status. (See if the Sensor is active. If the link is yellow, click on the cell to see the System Faults on the Sensor. For more information on this process, see McAfee Network Security Platform Manager Administration Guide.)
- In the Manager, click System and select the Domain to which the Sensor belongs. Then click Devices and select the Sensor. Then go to Setup | Monitoring Ports. Look at the color of the button(s) representing the ports on the Sensor, and check the color legend on the screen to see the status of the Sensor’s ports. (For more information on this process, see McAfee Network Security Platform Manager Administration Guide.)

If you have difficulty in troubleshooting the above, see McAfee Network Security Platform Troubleshooting Guide. Also, see McAfee Network Security Platform CLI Guide for a description of all available CLI commands.

How to change Sensor values

Changing certain values on the Sensor, like the Sensor’s name or Sensor IP address, require you to "break trust" between the Sensor and the Manager before you make the change, and then re-establish the communication with the Manager. Essentially, the Manager knows the Sensor by a specific set of information; if you want to change any of it, you must re-establish the communication with the Manager.

Changing any of these values requires you to "break trust" with the Manager:

- Sensor name
  
  Changing a Sensor’s name requires you to delete it from the Manager and re-add it, or in other words, re-configure the Sensor from the beginning. For instructions, see Add the Sensor to Manager and then Configuring the Sensor.

- Sensor shared secret
- Manager IP
- Sensor IP and subnet mask

See also

Add a Sensor to the Manager on page 57  
Configure the Sensor on page 58
Change the Sensor IP or the Manager IP

Task

1. On the Sensor, type `deinstall`.
   This breaks the trust relationship with the Manager.

2. Type the command and the new value.
   For example, type `set manager IP 192.168.3.2`.

3. Type the Sensor Shared Secret. (This value must match the value set for the Sensor in the Manager interface.)
   For example, `set sensor sharedsecretkey`. The Sensor then prompts you to enter a shared secret key value. Type the shared secret key value at the prompt. The Sensor then prompts you to verify the value. Type the value again.

   The shared secret key value must be between 8 and 25 characters of ASCII text. The shared secret key value is case-sensitive. For example, `IPSkey123`.

4. If you changed the Sensor IP address, then you must reboot the Sensor.
   Type `reboot`. You must confirm that you want to reboot the Sensor.

How to add a secondary Manager IP

Note that this command is used to add an IP address for a second NIC in one Manager server; this is not a command to use to set up a Manager Disaster Recovery peer—or Secondary—Manager.

To add a secondary Manager IP,

On the Sensor, type `set manager secondary ip <A.B.C.D.>`

Specify a 32-bit address written as four eight-bit numbers separated by periods, where A, B, C or D represents an eight-bit number between 0-255.

For example, `set manager secondary ip 192.168.3.19`

Or

Type `set manager secondary ip <A:B:C:D:E:F:G:H>`

where `<A:B:C:D:E:F:G:H>` is a 128-bit address written as octet (eight groups) of four hexadecimal numbers, separated by colons. Each group (A, B, C, D etc.) is a group of hexadecimal numbers between 0000-FFFF.

For example: `set manager secondary ip 2001:0db8:8a2e:0000:0000:0000:0000:0111`

If one or more four-digit group(s) is 0000, the zeros may be omitted and replaced with two colons (::).

For example, `set manager secondary ip 2001:0db8:8a2e::0111`

Remove a secondary Manager IP

To remove a secondary Manager IP, type `deletemgrsecintf`
Configuration of devices using the Manager

This section discusses the concepts and configuration instructions for managing devices like the Sensors and the NTBA Appliance using the Manager resource tree.

The Devices page can be accessed from the menu bar of the Manager. This page allows you to manage the group of Network Security Sensors and/or NTBA Appliances integrated with the Manager. The configuration settings for a specific domain specified under the Global tab sets general rules that are applied by default to all physical devices added within the Manager. These added devices appear in the list of devices visible in the Device drop down. These devices adopt the parent domains' general rules.

See also
Deploy pending changes to a device on page 79

Contents
- Install Sensors using the wizard
- Possible actions from the device list nodes
- Specify proxy server for internet connectivity
- Configure NTP server
- Configure NTP server for a device

Install Sensors using the wizard

This section describes the Sensor Installation Wizard in detail and provides information on how to use the tool.

To get McAfee® Network Security Platform up and running, you need to add a Sensor to the Manager and configure them as well. The Sensor Installation Wizard guides you through the steps involved in adding and configuring Sensors. The Wizard enables you to complete the required steps in a sequence.

To use this feature, you need to have Super User role in the root admin domain.

You can use the wizard only to install Sensors to the root admin domain.
Supported Sensor models

The Sensor installation using the wizard supports the following models:

- You can install I-series and M-series Sensors using the wizard.

- For I series Sensors:
  - You can change port configuration (inline, tap, and span) and other configuration per port such as, full duplex, speed, and apply policy per port, and finally push configuration changes.

- For M series Sensors:
  - For an IPS Sensor, you can change port configuration (inline, tap and span) and other configuration per port such as, full duplex, speed, and apply policy per port and finally push configuration changes.

- This wizard does not support NTBA Appliance installation.

Add and configure Sensors

The process of adding and configuring a Sensor involves invoking the Sensor installation wizard, importing signature sets from a local directory, adding a Sensor to the Manager, assigning port configuration on a Sensor, pushing configuration to the Sensor, selecting the signature set update method, downloading the latest signature set, configuring the Sensor using the command line interface, applying policies to the interfaces on the Sensor, and viewing the Sensor installation summary page.

Start the device installation wizard

Task

1. From Manager, go to Devices | <Admin domain name> | Global | Add Device Wizard to invoke the Add New Device wizard.

   To exit the wizard at any time, click the Global tab.

2. Click Next.

Select a signature set update method

In the Choose signature set update method page, you can identify the latest signature set available on your Manager, and decide whether you need to download the latest signature set from the Update Server.

Task

1. Indicate how you want to obtain the latest signature set:

   - Importing Signature sets from a Local Directory – You can import the signature set into Manager from a local directory.

   - Downloading the latest Signature set from McAfee Update Server – You can download the latest signature set from McAfee® Network Security Update Server (Update Server).

   - Skip Update Server authentication and signature set download – Use this option to continue with the default signature set that you received along with the Manager installation.

   - The Choose signature set method page displays the version of the current signature set available on the Manager.

2. Click Next.
Tasks

- Download the latest signature set on page 65
- Import signature sets from a local directory on page 65

Download the latest signature set
To download the latest signature set from the Update Server:

Task
1. In the Choose signature set update method page, select McAfee Update Server option.
2. Click Next.
   - The Authentication page is displayed.
3. Enter the Customer ID and Customer password provided by McAfee.
4. Click Next.
   - The available signature sets are listed.
5. Select the required signature set version and then click Next.
   - The Signature set download status page is displayed.
6. Click Next after the download is complete.
   - After the signature set has been downloaded, the Add a Sensor page is displayed.

Import signature sets from a local directory
To import a signature set from a local directory

Task
1. In the Choose signature set update method page, select the Import signature set from local directory option.
2. Click Next.
   - The Import Attack Set page is displayed.
3. Click Browse to select the file from the directory.

4. Click Next.

The Import Status is displayed.

![Import Status window](image)

Figure 6-1 Import Status window

After the signature set has been pushed, the Add a Sensor page is displayed.

**Add a Sensor to the Manager**

To add a Sensor, perform the following steps:

**Task**


2. Enter relevant details in the Add New Device dialog.
   a. Enter the **Device Name**.
      The Sensor name must begin with a letter. The maximum length of the name is 25 characters.
   b. Enter the **Sensor Type**, **IPS Sensor**, **Virtual HIP Sensor**, **NTBA Appliance**, or **Load Balancer**.
   c. Enter the **Shared Secret**. Re-enter to confirm.
      The shared secret must be a minimum of 8 characters and maximum of 25 characters in length. The key cannot start with an exclamation mark nor can have any spaces. The parameters that you can use to define the key are:
      - 26 alphabets: upper and lower case (a, b, c, ..., z and A, B, C, ..., Z)
      - 10 digits: 0 1 2 3 4 5 6 7 8 9
      - 32 symbols: ~ ! @ # $ % ^ & * ( ) _ + - = [ ] { } \ | ; : " ' , . <? /

   The Sensor name and shared secret key that you enter in the Manager must be identical to the shared secret that you will later enter during physical installation/initialization of the Sensor (using CLI). If not, the Sensor will not be able to register itself with Manager.

3. Select the **Updating Mode**, either **Online** or **Offline**.
   Selecting **Offline** enables Offline Sensor update. **Online** is the default mode.
4 Enter Contact Information and Location (optional)

5 Click Save.

6 An information box confirms successful addition of Sensor.

7 Click Next.

8 The new Sensor is listed in the Sensors page.

   You can select the Sensor and click Edit to edit the Sensor settings.

**Configure the Sensor using CLI**

**Task**

1 Open a HyperTerminal session to configure the Sensor. This task is performed to establish the trust with the Sensor.

   ![CLI window](image)

   **Figure 6-2 CLI window**

   For instructions, see Cabling the Console Port, *McAfee Network Security Platform Sensor Product Guide* for your Sensor model.

2 At the login prompt, log on to the Sensor using the default username admin and password admin123.

   McAfee strongly recommends that you change the default password later for security purposes.

3 Set the name of the Sensor. At the prompt, type: set Sensor name <WORD>

   Example: set Sensor name Engineering_Sensor1.

   The Sensor name is a case-sensitive alphanumeric character string up to 25 characters. The string can include hyphens, underscores, and periods, and must begin with a letter.
4 Set the IP address and subnet mask of the Sensor. At the prompt, type: set Sensor ip <A.B.C.D> <E.F.G.H>
Specify a 32-bit address written as four octets separated by periods: X.X.X.X, where X is a number between 0-255. For example: set Sensor ip 192.34.2.8 255.255.255.0

Setting the IP address for the first time—that is, during the initial configuration of the Sensor—does not require a Sensor reboot. Subsequent changes to the IP address will, however, require that you reboot the Sensor for the change to take effect. If a reboot is necessary, the CLI will prompt you to do so. For information on rebooting, see the McAfee Network Security Platform Troubleshooting Guide.

5 If the Sensor is not on the same network as Manager, set the address of the default gateway. At the prompt, type: set Sensor gateway <A.B.C.D>
Use the same convention as the one for Sensor IP address. For example: set Sensor gateway 192.34.2.8.

6 Set the IP address of Manager server. At the prompt, type:
set Manager ip <A.B.C.D>
Use the same convention as the one for Sensor IP address. Example: set Manager ip 192.34.3.2.

7 Ping Manager from the Sensor to determine if your configuration settings to this point have successfully established the Sensor on the network. At the prompt, type:
ping <manager IP address>
If the ping is successful, continue with the following steps. If not, type show to verify your configuration information and check to ensure that all information is correct. If you run into any difficulties, see the McAfee Network Security Platform Troubleshooting Guide.

8 Set the shared key value for the Sensor. This value is used to establish a trust relationship between the Sensor and Manager. At the prompt, type:
set Sensor sharedsecretkey
The Sensor then prompts you to enter a shared secret key value. Type the shared secret key value at the prompt. The Sensor then prompts you to verify the value. Type the value again.

The shared secret key value must be between 8 and 25 characters of ASCII text. The shared secret key value is case-sensitive. Example: IPSkey123

9 (Optional, but recommended) Change the Sensor password. At the prompt, type:
passwd.
The Sensor prompts you to enter the new password and prompts you for the old password. The password must be a minimum of 8 characters in length, and can be up to 25 characters long. The characters that can be used while setting a new password are:
- 26 alphabets: both upper and lower case are supported (a,b,c,...z and A, B, C,...Z)
- 10 digits: 0 1 2 3 4 5 6 7 8 9
- Symbols: ~ ` ! @ # $ % ^ & * ( ) _ + - = [ ] \ { } | ; : " ' , . < /

The question mark (?) symbol is not supported in a Sensor password.

10 To exit the session, type exit.
11 Switch back to the Sensor Installation Wizard to continue with the Sensor installation. At this point you are on the Sensor Discovery page.

12 Click Next.

**View the discovery status of a Sensor**

The Sensor [Sensor name] Discovery Status page shows whether connection has been established between the Sensor and the Manager.

If the Sensor has not been added or if you had entered an incorrect shared secret key, then click Re-try discovery and provide the correct details.

The action buttons on the page is described as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back</td>
<td>Brings you to the Add Sensor page.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Cancels the discovery process of a Sensor in the network.</td>
</tr>
<tr>
<td>Re-try Discovery</td>
<td>Starts the discovery process once again.</td>
</tr>
<tr>
<td>Next</td>
<td>Moves you to the Edit Port configuration to Sensor page to configure port for a Sensor.</td>
</tr>
</tbody>
</table>

**Assign port configuration on a Sensor**

The Edit Port Configuration page is displayed.

You can edit the configuration for a particular port. To edit a port’s configuration:

**Task**

1 Select a port from the list of ports displayed.

2 Click Edit.

3 Select the mode of operation for the port from the Operation Mode list:
   - Inline Fail-Open
   - Internal Tap
   - Span or Hub
   - Inline Fail-Close

4 Specify whether you want to connect the port from inside or outside using the Port Connected Network list.
   - Port A (Inside) Port B (Outside)
   - Port A (Outside) Port B (Inside)
   - Not specified

5 Click Next.

The Assign policies to Sensor page is displayed. Select the policy from the list of policies and apply them to the Sensor.
Apply policies to the interfaces on the Sensor

Task
1. Select a policy and apply them to Sensor, default policy applied is Default Inline IPS policy.
2. If required, change the applied policies for the interfaces on the Sensor.

   All interfaces inherit a policy from the Sensor by default. The Sensor inherits the policy from the parent admin domain, and takes the default Inline IPS policy by default.

3. Click Next.
   The Signature Set Push Status page is displayed.

Push configuration to the Sensor

Task
1. Click Next to push the configuration information to the Sensor.
   The Signature Set Push Status page is displayed.
2. Click Next.
   The Sensor Installation Summary page is displayed.

View the Sensor installation summary page

Once the Sensor has been successfully installed, the Sensor Installation Summary page is displayed.

The following fields are displayed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor Name</td>
<td>Name of the Sensor</td>
</tr>
<tr>
<td>Sensor Model</td>
<td>Model of Sensor</td>
</tr>
<tr>
<td>Trust Status</td>
<td>The status of the trust: established or not</td>
</tr>
<tr>
<td>Applied Signature Set</td>
<td>Signature set version number applied to the Sensor</td>
</tr>
<tr>
<td>Interface Name</td>
<td>Ports on the Sensor</td>
</tr>
<tr>
<td>Operation Status</td>
<td>Status of the port: enabled or disabled</td>
</tr>
<tr>
<td>IP</td>
<td>Set the IP address of the Sensor</td>
</tr>
<tr>
<td>Mask</td>
<td>Set the subnet mask of the Sensor</td>
</tr>
<tr>
<td>Gateway</td>
<td>Set the address of the default gateway</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Set the VLAN ID of the monitoring ports.</td>
</tr>
</tbody>
</table>

Task
1. Click Done.
   Installation Wizard welcome page is displayed to enable you to install another Sensor.
2. Repeat steps to add and configure another Sensor.
3. Click Resource Tree in the Resource pane to exit the wizard.
Add and configure the XC Clusters

An XC Cluster in McAfee® Network Security Platform, comprising an XC-240 Load Balancer and M-8000XC Sensors, functions like a single virtual Sensor. The XC Cluster handles traffic at wire-speed, efficiently inspects, detects and prevents intrusions, misuse, denial of service (DoS) attacks, and distributed denial of service (DDoS) attacks with a high degree of accuracy. It enables high traffic loads to be processed by distributing the traffic flow to multiple Sensors to avoid congestion providing a maximum throughput of 80 Gbps.

Once deployed, XC Clusters are configured and managed through the command line and the Manager.

For more information, see McAfee Network Security Platform XC Cluster Administration Guide.

Possible actions from the device list nodes

The four Device List node tabs are Devices (Device List), Configuration Update (download configuration to devices), Software Upgrade, and Failover Pairs. The following actions are possible through these tabs:

- Managing Devices — Add devices to the Manager; accept communication from an initialized, physically installed and network-connected devices like IPS Sensors, NTBA Appliances or virtual HIP Sensors to the Manager.

- Updating the configuration of all devices — All changes done via the Configuration page that apply to your Sensors are not pushed until you perform a Device List | Configuration Update | Update (all Sensors in a domain) or Device List | Sensor_Name | Configuration Update | Update (single Sensor) action.

- Updating software to all devices — Download software and signature files from the Manager via McAfee® Network Security Update Server [formerly IPS Update Server]

- Creating Failover Pairs — Pair two devices for failover operation.
Options available in the devices page

The **Devices** action presents a read-only view of operational and status details for all the devices added under the devices node. Each installed device is displayed with its corresponding type, operating ports, operating mode, administrative status, and Operational Status.

Using this page, you can configure physical devices like IPS Sensors, NTBA Appliance or Load Balancer to the Manager. Once you add a device on the Device List node, you must establish between the device and the Manager by executing the setup CLI command.

You can use this page to also add virtual HIP Sensors to the Manager. The trust establishment for the Virtual HIP Sensor is done using McAfee ePO™ console.

See also

*Edit device settings on page 78*

Add a device using the wizard

Adding a device to the Manager enables the Manager to accept communication from a physically installed and network-connected device. Once communication has been established, the Manager allows editing of the device configuration. The alert data is available in the Threat Analyzer and Report queries.

> McAfee recommends adding a device to the Manager first. The **Add Device Wizard** will be displayed once the **Manager Initialization Wizard** is completed.
To add a device to the Manager:

**Task**

1. Click **Devices | <Admin domain name> | Global | Wizards | Add Device**.

![Add Device link under the Wizard node](image)

**Figure 6-4 Add Device link under the Wizard node**

The **Add Device** page is displayed.

![Add Device page](image)

**Figure 6-5 Add Device page**

The **Preparation** page is displayed.

2. Click **Next**.

The **Add New Device** page is displayed.

3. Enter the device name.

   - **The Name** must begin with a letter and can contain alphanumeric characters, hyphens, underscores and periods. The length of the name is not configurable.

4. Select the **Device Type** as **IPS Sensor**.
5 Enter **Shared Secret** (repeat at **Confirm Shared Secret**).

The shared secret must be a minimum of 8 characters in length: the length of the shared secret is not configurable. The shared secret cannot start with an exclamation mark or have any spaces. The characters that can be used while creating a shared secret are as follows:

- 26 alpha: upper and lower case (a,b,c,...z and A, B, C,...Z)
- 10 digits: 0 1 2 3 4 5 6 7 8 9
- 32 symbols: ~ ` ! @ # $ % ^ & * ( ) _ + - = \ [ ] { } \ | ; : " ' , . <? />

**IMPORTANT:** The device name and shared secret are case-sensitive. The **Device Name** and **Shared Secret** must also be entered on the device command line interface (CLI) during physical installation and initialization. If not, the device will not be able to register itself with the Manager.

6 Select **Updating Mode** as **Online** or **Offline**. **Online** is the default mode.

**Devices with Online update mode will have the signature set/software directly pushed to the devices. Devices for which you want the signature set/software to be manually pushed can be done by selecting the update mode as Offline.**

7 [Optional] Enter the **Contact Information** and **Location**.

8 Click **Next**. The **Trust Establishment** page is displayed.

9 Follow the instructions on the page to complete the command line interface (CLI) setup and click **Check Trust**.

**Using the command line interface (CLI), enter the necessary information for the device identification and communication as described in Configure the Sensor on page 58. If you set up the device first, you will need to return to the device after the Manager addition to reset the shared secret key and begin device-to-Manager communication.**

10 Click **Next**. The **Port Settings** page is displayed.

11 Make the necessary changes and click **Next**.

The **Policy Assignments** page is displayed.

12 Make the necessary changes and click **Next**.

The **DNS Settings** page is displayed.

**The DNS Settings page is applicable only to M-series Sensor (software version above 7.0).**

13 Configure the DNS server details. Click **Next**.

The **Application Identification** page is displayed.

**The Application Identification page is applicable only to M-series Sensor (software version above 7.0).**

14 Select the **Enable Application Identifier?** check box for the required ports. Click **Next**.
15 Click **Update** to start update.

The **Update Configuration** page is displayed.

16 Click **Finish**.

You will now be able to see the device when you click on the **Device** drop-down.

![Device added to the Device drop-down](image)

**Figure 6-6 Device added to the Device drop-down**

**Add the NTBA Appliance to the Manager**

Adding an NTBA Appliance to the Manager enables the Manager to accept communication from a physically installed and network-connected Appliance. After communication has been established, the Manager allows editing of the Appliance configuration. The alert data is available in the Threat Analyzer and Report queries.

You can add a device by selecting **Devices** | **<Admin Domain Name>** | **Global** | **Add and Remove Devices** but it is recommended to use the **Add Device Wizard** to add all devices (except Virtual HIP Sensors) and to establish the trust between the Manager and the device.
Task

1. The Add Device Wizard window is displayed after the Manager Initialization Wizard is completed.

   ![McAfee recommends adding an Appliance to the Manager first.]

Select Devices | <Admin Domain Name> | Global | Add Device Wizard.

The Preparation page is displayed.

![Figure 6-7  Add Device Wizard](image)

2. Click Next.

   The Add New Device page is displayed.

3. Enter the device name.

   The name must begin with a letter and can contain alphanumeric characters, hyphens, underscores and periods. The length of the name is not configurable.

4. Select the Device Type as NTBA Appliance.

5. Enter the Shared Secret (repeat at Confirm Shared Secret).

   The device name and shared secret are case-sensitive. The Device Name and Shared Secret must also be entered on the device command line interface (CLI) during physical installation and initialization. If not, the Appliance will not be able to register itself with the Manager.

   The shared secret must be a minimum of 8 characters in length: the length of the shared secret is not configurable. The shared secret cannot start with an exclamation mark or have any spaces. The characters that can be used while creating a shared secret are as follows:

   - 26 alpha: upper and lower case (a,b,c,...z and A, B, C,...Z)
   - 10 digits: 0 1 2 3 4 5 6 7 8 9
   - 32 symbols: ~ ` ! @ # $ % ^ & * ( ) _ + - = [ ] \ | ; : " ' , . <? /

6. Select the updating mode.
7 [Optional] Enter the Contact Information and Location.

8 Click Next.

The Trust Establishment page is displayed.

9 Follow the instructions on the page to complete the command line interface (CLI) setup and click Check Trust.

Using the command line interface (CLI), enter the necessary information for the Appliance identification and communication as described in "Configure the Sensor". If you set up the Appliance first, you will need to return to the Appliance after the Manager addition to reset the shared secret key and begin Appliance-to-Manager communication.

10 Click Next.

The Next button will be enabled once the trust between the Appliance and the Manager is established.

The Port Settings page is displayed.

11 Make the necessary changes and click Next.

The General Settings page is displayed.

12 Define essential NTBA Appliance settings, including flow record listening port and Ethernet port IP settings. Click Next.

The DNS Settings page is displayed.

The DNS Settings page is applicable only to M-series (software version above 7.0) and NS-series Sensors.

13 Configure the DNS server details. Click Next.

The Exporters page is displayed. You can add a new exporter or edit the existing one.

14 Define exporters that will forward records to the NBA Sensor for processing and click Next.

The Inside Zones page is displayed. You can add a new inside zone or edit the existing one.

15 Define inside zones and click Next.

The Outside Zones page is displayed. You can add a new outside zone or edit the existing one.

16 Define outside zones and click Next.

The Active Device Profiling page appears.

17 Select the Active Device Profiling checkbox and click Next.

The Update Configuration page is displayed.

18 Click Update to start update.

The Update Configuration page is displayed.
19  Click Finish.

The NTBA Appliance appears added under the Device drop-down list in the Devices tab. It also appears in the Add and Remove Devices in the Global tab.

![Add and Remove Devices](image)

**Figure 6-8 Add and Remove Devices**

20  To edit or delete an existing device, click Edit or Delete.

21  Skip the Chapter, *Setting up Virtual NTBA Appliance on an ESX server*, and proceed to Chapter, *Configuring NTBA Appliance settings*.

**Edit device settings**

You can edit all the parameters except Device Type. The shared secret is the most important to note. Changing the shared secret can be performed in the event you want to re-secure your system's integrity.

McAfee recommends changing the Shared Secret from the Manager first. You do not have to immediately change the shared secret in the device CLI; the Manager and the device will continue to communicate. However, when you update the Shared Secret on the CLI, you must type the same value as entered in this action.

To edit a device, do the following:

**Task**

1  Select Devices | <Admin Domain> | Global | Add and Remove Devices.

2  Select the device.

   To edit Virtual Security Systems, you must use the Intel® Security Controller web application.

3  Click Edit.

4  Make the required changes.

5  Click Save to save the changes; click Cancel to abort.

**Delete a device configuration**

To delete a previously added device, select the device from the by going to Devices | <Admin Domain> | Global | Add and Remove Devices and click Delete. Confirm the deletion by clicking OK.
Notes:

- Do not delete the device from the Manager if you plan to generate reports with data specific to the device.
- If the device is in the middle of active communication with the database, deleting the device may not be successful (the device still appears in the Resource Tree). If you experience this problem, check your device to make sure communication to the Manager is quiet, then re-attempt the delete action.

Deleting a deployed Virtual Security System, seriously damages the IPS service deployed through Intel® Security Controller. Before you delete a Virtual Security System, make sure you uninstalled the IPS service in VMware NSX and then deleted the corresponding distributed appliance and manager connector in Intel® Security Controller.

Deploy pending changes to a device

When you make any configuration changes, or policy changes on the Manager, or a new/updated signature set is available from McAfee, you must apply these updates to the devices (such as Sensors and NTBA Appliances) in your deployment for the changes to take effect.

Note the following:

- Configuration changes such as port configuration, non-standard ports and interface traffic types are updated regardless of the changes made to the Sensor, interface/ subinterface.
- NTBA configuration updates refer to the changes done in the various tabs of the Devices node.
- Policy changes are updated on the Sensor or NTBA Appliance in case of a newly applied policy, or changes made to the current enforced policy.
- Signature updates contain new and/or modified signatures that can be applied to the latest attacks.

You can deploy the configuration changes to all the devices in the admin domain from the Global tab. The navigation path for this is Devices | <Admin Domain Name> | Global | Deploy Pending Changes.

Alternatively, you can deploy the configuration changes at a device level by selecting Devices | <Admin Domain Name> | Devices | <Device name> | Deploy Pending Changes. In this case, the Deploy Pending Changes option is available in the menu only if the device is active.
**Task**

1. Select Devices | <Admin Domain Name> | Global | Deploy Pending Changes.

The Deploy Pending Changes page is displayed.

![Deploy Pending Changes page](image)

2. Click Deploy.

The Manager processes these updates in three stages — Queued, Deploying, Completed — and displays the current stage in the Status Column.

![Configuration update](image)
### Status | Description
--- | ---
Queued | The Queued status indicates that the Manager is preparing to deploy updates to the devices. If more than one device is being updated, devices are updated one at a time until all downloads are complete. If you want to cancel the updates for certain devices, click the X. Consider the following:
- The deployment of the configuration changes or signature file updates can be cancelled for bulk updates only.
- Updates cannot be cancelled when deployed for individual devices.
- After you click **Deploy**, wait for five seconds before you start cancelling the updates for devices.
- Once cancelled, the checkbox is deselected, suggesting that the update was cancelled. There is no status change to indicate the cancellation of an update.

Deploying | In this state, the configuration changes are applied to the devices. There is no option to abort the update process for devices in which the deployment of updates are already in progress. When the deployment is cancelled for any device, the item will still be selected for future updates unless it is explicitly deselected.

Completed | Shows that all the configuration changes have been updated for the devices.

3 Click **Offline Update Files** to view and export the deployment changes file to offline Sensors. The changes can then be deployed to the Sensors manually using the CLI command window.

4 Click **Refresh** to refresh the page and the status of the deployment.

5 Click **Clear Status** to clear the status column in the UI.

*Clearing the status does not cancel the deployment. The update process will be running in the background.*

### See also
- *Possible actions from the device list nodes on page 71*
- *Configuration of devices using the Manager on page 4*

### Deploy pending changes to a device
When you make any configuration changes, or policy changes on the Manager, or a new/updated signature set is available from McAfee, you must apply these updates to the devices (such as Sensors and NTBA Appliances) in your deployment for the changes to take effect.

Note the following:

- Configuration changes such as port configuration, non-standard ports and interface traffic types are updated regardless of the changes made to the Sensor, interface/ subinterface.
- NTBA configuration updates refer to the changes done in the various tabs of the Devices node.
- Policy changes are updated on the Sensor or NTBA Appliance in case of a newly applied policy, or changes made to the current enforced policy.
- Signature updates contain new and/or modified signatures that can be applied to the latest attacks.

You can deploy the configuration changes to all the devices in the admin domain from the Global tab. The navigation path for this is **Devices** | **<Admin Domain Name>** | **Global** | **Deploy Pending Changes**.

Alternatively, you can deploy the configuration changes at a device level by selecting **Devices** | **<Admin Domain Name>** | **Devices** | **<Device name>** | **Deploy Pending Changes**. In this case, the **Deploy Pending Changes** option is available in the menu only if the device is active.
Task

1. Select Devices | <Admin Domain Name> | Global | Deploy Pending Changes.

The Deploy Pending Changes page is displayed.

![Deploy Pending Changes page](image)

The columns in the table are as follows:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Unique name of each device</td>
</tr>
<tr>
<td>Last Update</td>
<td>Last day and time device configuration was updated.</td>
</tr>
<tr>
<td>Updating Mode</td>
<td>Online or offline update mechanism selected for the device.</td>
</tr>
<tr>
<td>Pending Changes</td>
<td>Summary of changes that have been made</td>
</tr>
<tr>
<td>Deploy</td>
<td>A selected checkbox indicates that the device is to be updated for any configuration change other than those related to SSL key management. This check-box will include updates for configuration and signature set, botnet detectors, and Gateway Anti-Malware.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status of the Sensor during update</td>
</tr>
</tbody>
</table>

2. Click Deploy.
The Manager processes these updates in three stages — Queued, Deploying, Completed — and displays the current stage in the **Status** Column.

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Last Update</th>
<th>Mode</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 6-12 Configuration update**

**Status** | **Description**
--- | ---
**Queued** | The **Queued** status indicates that the Manager is preparing to deploy updates to the devices. If more than one device is being updated, devices are updated one at a time until all downloads are complete. If you want to cancel the updates for certain devices, click the X. Consider the following:
- The deployment of the configuration changes or signature file updates can be cancelled for bulk updates only.
- Updates cannot be cancelled when deployed for individual devices.
- After you click **Deploy**, wait for five seconds before you start cancelling the updates for devices.
- Once cancelled, the checkbox is deselected, suggesting that the update was cancelled. There is no status change to indicate the cancellation of an update.

**Deploying** | In this state, the configuration changes are applied to the devices. There is no option to abort the update process for devices in which the deployment of updates are already in progress. When the deployment is cancelled for any device, the item will still be selected for future updates unless it is explicitly deselected.

**Completed** | Shows that all the configuration changes have been updated for the devices.

3. Click **Offline Update Files** to view and export the deployment changes file to offline Sensors. The changes can then be deployed to the Sensors manually using the CLI command window.

4. Click **Refresh** to refresh the page and the status of the deployment.

5. Click **Clear Status** to clear the status column in the UI.

> Clearing the status does not cancel the deployment. The update process will be running in the background.

**Update the latest software images on all devices**

Going to **Devices | <Admin Domain Name> | Global | Deploy Device Software** enables an on-demand download of the latest software updates from your Manager to all of your Sensors under a Device List node. If more than one version is available, select the most recent version (that with the highest version number). If multiple versions are available for download, such as 7.1.1.4, 7.1.1.5, and 7.1.1.6, and
you select 7.1.1.6, previous versions (7.1.1.4 and 7.1.1.5) are still available for download. However, if you upgrade to a new major version (7.1.x.x), previous major versions (6.1.x.x) are not available. The latest version of software always contains the changes in every previous release. The Manager also provides an option to concurrently perform the Sensor upgrade by selecting the Sensors in the Upgrade field under Device List | Software Upgrade.

After software download to your Sensors, you must reboot all updated Sensors. To download a software update, do the following:

**Task**

1. **Select Devices | <Admin Domain Name> | Global | Deploy Device Software.**

   The Download Software to Devices page is displayed.

2. **Select the New Version to be downloaded to the Sensor.**

   ![Figure 6-13 Software Upgrade window](image)

   - To select a Sensor for update, select the check boxes (for the specific Sensor) in the Upgrade column.

   - To select a Sensor for reboot, select the check boxes (for the specific Sensor) in the Reboot column.

   By default the Reboot option is disabled. It gets enabled only after you select the Sensor(s) in the Upgrade column. This option triggers a full reboot even if hitless reboot option is available for the corresponding Sensors. The Reboot option can also be disabled if required.

3. **Click the Upgrade button to initiate the process.**

4. **The Offline Upgrade Files is used to update and export Offline Sensors.**

   - **Refresh** enables you to see the new Sensor software version after reboot.

   - **Clear Status** is used for clearing the cached status.

**See also**

- Possible actions from the device list nodes on page 71
- Download software update files for offline devices on page 84

**Download software update files for offline devices**

Some users manage devices that are connected to the Manager across very low bandwidth links such as dial-up links. In addition to the low bandwidth, these links may also be intermittent and may corrupt a large file being downloaded. To alleviate this issue, the Manager provides an option to generate and store the signature set file and/or software update files for the device on a CD is provided. Users can ship the CD to the remote location and then use a TFTP server to transfer the file onto the device.
The update files are encrypted using a symmetric key cipher. The download consists of the encrypted signature set and/or image file and a meta information file that contains the details of the download created. These three files are zipped together to create a download file that can be saved on CD and later be uploaded to the device via TFTP. This is illustrated as follows:

**Figure 6-14  Encryption process**

**See also**
- Configure a new device for offline signature set update on page 85
- Update configuration for offline devices on page 86
- Update software for offline devices on page 88
- Configure an existing device for offline signature set update on page 86
- Export software for offline devices on page 87
- Export software for offline devices on page 89
- Update the latest software images on all devices on page 83

**Configure a new device for offline signature set update**

The Manager provides an option to generate and store the signature set and/or device image file on an application directory. You can export the generated file to a directory or a CD, manually ship the CD to a remote location, and then use a TFTP server to transfer the file onto the device.

You can select the device Update Mechanism mode while adding a new device. By default, all devices added to the Manager have the update mode as Online. Devices with Online update mode will have the signature set / software directly pushed to the devices as it has been done in the past. Devices for which you want the signature set / software to be manually pushed can be done by selecting the update mode as Offline. You can edit the update mode later, if required.

Follow this procedure to configure a new device for Offline update:

**Task**

1. Click Devices | <Admin Domain> | Global | Add and Remove Devices

2. Click New.
   
   The Add New Device page is displayed.
3. Enter a name against Device Name, Select IPS Sensor against Device Type, Enter Shared Secret and Confirm Shared Secret.

4. Select Offline under Updating Mode and click Save.
   
The device is configured for Offline update.

   - The Updating Mode configured on the Primary device of the Fail Over - Pair determines the signature file generation for download.
   - If the Primary device is configured for Offline Updating Mode, then two individual signature files are generated for Primary and Secondary devices, irrespective of the Secondary device configuration.
   - If the Primary device is configured for Online Updating Mode, then signature file will be downloaded online to both devices, irrespective of the Secondary device configuration.

See also

*Download software update files for offline devices on page 84*

### Configure an existing device for offline signature set update

Follow this procedure to configure an existing device for offline signature set update:

**Task**

1. Click Devices | <Admin Domain> | Global | Add and Remove Devices to view the list of devices configured.

2. Select the device and click Edit. Select Offline against Updating Mode and click Save.

3. The information box confirms a successful edit. The device is configured for Offline update.

   - The Updating Mode configured on the Primary device of the Failover - Pair determines the signature file generation for download.
   - If the Primary device is configured for Offline Updating Mode, then two individual signature files are generated for Primary and Secondary devices, irrespective of the Secondary device configuration.
   - If the Primary device is configured for Online Updating Mode, then signature file will be downloaded online to both devices, irrespective of the Secondary device configuration.

See also

*Download software update files for offline devices on page 84*

### Update configuration for offline devices

Follow this procedure for updating device configuration for offline devices:

**Task**

1. Click Devices | <Admin Domain> | Global | Deploy Configuration Changes.
The list of devices for which configuration can be downloaded are listed under Configuration Update. Select the Configuration Update check box against the device listed as Offline in the Updating Mode column. Click Update.

The update is listed under Sigfile for Offline Sensors in the Configuration Update tab on the Device List node and is ready for export.

- The Updating Mode configured on the Primary device of the Fail Over - Pair determines the signature file generation for download.
- If the Primary device is configured for OfflineUpdating Mode, then two individual signature files are generated for Primary and Secondary device, irrespective of the secondary device configuration.
- If the Primary device is configured for OnlineUpdating Mode, then signature file will be downloaded online to both devices, irrespective of the secondary device configuration.

See also
Download software update files for offline devices on page 84

Export software for offline devices
Follow this procedure to export a signature set for offline devices:

Task

![Figure 6-15 IPS Sensors tab](image)

2. Select radio button under the Export File column in the device listed under Available Configuration Files for Offline Devices. Click Export.

3. Select the Save File option. Click OK and save the signature file in the desired location in the local machine.

Tasks
- Perform an offline download of the signature set on page 87

See also
Download software update files for offline devices on page 84

Perform an offline download of the signature set
To perform an offline download of the signature set:

Task
1. Copy the signature set to the tftp server.
2. Connect to the device through CLI and configure the tftp server IP.
3 Execute the loadconfiguration signature filename.

4 Once the signature file is copied on to the device, check with "downloadstatus" command in the CLI to get the status.

**Update software for offline devices**

Follow this procedure for updating device configuration for offline devices:

**Task**

1 Click Devices | <Admin Domain> | Global | Deploy Device Software.

![Figure 6-16 Configuration Update sub-tab](image)

2 The list of devices for which software can be downloaded are listed under Deploy Device Software table. Select the checkbox against the device listed as Offline in the Upgrade column. Click Update.

![Figure 6-17 Download Status dialog](image)

3 The update is listed under Available Configuration Files for Offline Devices in the Configuration Update table is ready for export.

**See also**

*Download software update files for offline devices on page 84*
Export software for offline devices

Follow this procedure to export a signature set for offline devices:

**Task**

1. Click Devices | <Admin Domain> | Devices | <Device Name> | Maintenance | Export Configuration.

![Figure 6-18  Device List tab](image)

2. Select all required configuration that you wish to export and click Export column.

3. Select the Save File option. Click OK and save the device software in the desired location.

**Tasks**

- Import software for offline devices on page 89

**See also**

Download software update files for offline devices on page 84

Import software for offline devices

To perform an offline download of the device software:

**Task**

1. Set up the Manager and device.

2. Import the device image jar file on to the Manager, using Manage | Updating | Manual Import.

3. Click Deploy Device Software, which is also located under the Updating tab.

4. Select the device and image to apply and click Upgrade. The offline image is generated in the same page below, under Available Upgrade Files for Offline Devices.

5. Execute the loadconfiguration imagefile name from the CLI.

6. Once the imagefile copied on to the device (it takes some time), check with "downloadstatus" command in the CLI to get the status.

7. Reboot the device on successful loading of the image.

Malware engine updates

Among the malware scanning engines present on the Sensor, the Gateway Anti-Malware Engine and the Blacklist can be updated through the intervention of the security administrator. Updates for these engines can be carried out independent of the Sensor software version.

However, for Gateway Anti-Malware, you must be aware about which versions of the malware engines are compatible with specific Sensor and Manager versions. Refer to Gateway Anti-Malware Engine within the section, How an Advanced Malware policy works.
**Gateway Anti-Malware update**

The Gateway Anti-Malware Engine, running either on an NS-series Sensor or on an NTBA appliance, can be updated from the Manager in the same way that you perform configuration and device software updates. You can set up automatic updates in the Manager for this engine using one of the methods mentioned.

**Set up automatic updates for Gateway Anti-Malware Engine for a domain**

**Before you begin**

- Make sure that you have configured a DNS server for the domain to allow Sensors attached to this domain to download Gateway Anti-Malware Engine updates. If you have not done so, go to Devices | <Admin_Domain_Name> | Global | Common Device Settings | Name Resolution to configure a DNS server.

- You must be using either an NS-series Sensor running Sensor software version 8.2 or above or an NTBA Appliance to use this engine.

An update comprises the following components:

- Gateway Anti-Malware DAT and Gateway Anti-Malware Engine
- Anti-Virus DAT
- Anti-Malware Engine

The update can either be an incremental update or a full update. The full update is approximately 150 Mb.

You can set up automatic updates for both these components using these steps. If you do not want to set up automatic updates, you can use the existing process for manual updates.

**Task**

1. Click Devices | <Admin_Domain_Name> | Global | Common Device Settings | GAM Updating. The GAM Updating page appears.

2. Select Enable Automatic Updating?

   ![Warning](image)

   **Figure 6-19 Notification to configure a DNS server**

   If you have not configured a DNS server for this domain, you will receive a notification prompting you to do so.

3. Click the Update Interval drop-down.

   The range of the update interval is between 2 hours and 24 hours since McAfee provides updates several times in a day.

4. Click Save to complete the configuration.

You have now set up automatic updates for all devices that run Gateway Anti-Malware Engine in the domain.
Set up automatic updates for Gateway Anti-Malware Engine for a device

Before you begin

- Make sure that you have configured a DNS server for this device to allow the Sensor to download Gateway Anti-Malware Engine updates. If you have not done so, go to Devices | <Admin_Domain_Name> | Devices | <Device_Name> | Setup | Name Resolution to configure a DNS server.
- You must be using either an NS-series Sensor running Sensor software version 8.2 or above or an NTBA Appliance to use this engine.

An update comprises the following components:

- Gateway Anti-Malware DAT and Gateway Anti-Malware Engine
- Anti-Virus DAT
- Anti-Malware Engine

The update can either be an incremental update or a full update. The full update is approximately 150 Mb.

You can use these steps to set up automatic updates for both these components. If you do not want to set up automatic updates, you can use the existing process for manual updates.

This page displays a grid that mentions that active version and latest available version of each component. If you are using the latest version the circle is green. If a newer version is available, the circle is colored red.

Task

1. Click Devices | <Admin_Domain_Name> | Devices | <Device_Name> | Setup | GAM Updating.

   The GAM Updating page appears.

2. You can choose to inherit settings of the domain by selecting the check-box.

   If you do not select this option, you can customize update settings for this device.

3. Select Enable Automatic Updating?

   ![Warning]

   Automatic updating requires name resolution, however, name resolution is currently disabled for this admin domain.

   ![OK]

   Figure 6-20 Notification to configure a DNS server

   If you have not configured a DNS server for this device, you will receive a notification prompting you to do so.

4. Click the Update Interval drop-down.

   The range of the update interval is between 2 hours and 24 hours since McAfee provides updates several times in a day.
5 Click **Save** to complete the configuration.

![GAM Updating page shows versions for individual items](image)

You have now set up automatic Gateway Anti-Malware Engine updates for this Sensor.

**Update Gateway Anti-Malware Engine manually**

If you want to update the Gateway Anti-Malware Engine for an offline Sensor, you will need to manually download the appropriate software version and import it into the Manager.

It is important that you download a compatible version of Gateway Anti-Malware Engine files to make sure the update is successful. To ascertain which software versions are compatible with which versions of the Sensor software, refer to Gateway Anti-Malware Engine within the section, *How an Advanced Malware policy works*.

Perform the steps listed below to manually download the Gateway Anti-Malware Engine update files and deploy them to your Sensor.

**Task**

1. Using a recent version of your browser, go to the Gateway Anti-Malware Update Server URL: [https://contentsecurity.mcafee.com/update](https://contentsecurity.mcafee.com/update).

2. On the page that appears, review the terms and conditions and select the **I accept the terms and conditions** checkbox, and click **Next Step**.

**Manual Update**

**Download Update Package for McAfee® Products**

If you have a valid licensed McAfee product you can manually download personalized update packages. These update packages can be used for a manual import into your McAfee product. Please finish the following steps to start the generation of your personalized update package.

**Step 1/4**

**Terms and Conditions**

*IMPORTANT NOTICE - PLEASE READ CAREFULLY*

*BY ACCEPTING, I AGREE WITH THE FOLLOWING TERMS AND CONDITIONS*

Product updates and upgrades, including engine and DAF updates, are intended only for McAfee customers with a valid Technical Support Agreement.

- I accept the terms and conditions

You are routed to the next page where you will need to select the appropriate McAfee product.
3 On this page, click the drop-down to select McAfee Network Security Appliance, and click Next Step.

Manual Update

Download Update Package for McAfee® Products

If you have a valid licensed McAfee product you can manually download personalized update packages. These update packages can be used for a manual import into your McAfee product. Please finish the following steps to start the generation of your personalized update package.

Step 2/4

Please select your McAfee product.

McAfee Network Security Appliance

Cancel Previous Step Next Step

You are routed to the next page where you must enter the appropriate version of Sensor software you are using.

4 Enter 8.2 and the build number of the Sensor software, and click Next Step.

Manual Update

Download Update Package for McAfee® Products

If you have a valid licensed McAfee product you can manually download personalized update packages. These update packages can be used for a manual import into your McAfee product. Please finish the following steps to start the generation of your personalized update package.

Step 3/4

"McAfee Network Security Appliance" version
8.2
"McAfee Network Security Appliance" build number
8.2.5.145

The success or failure of the update will vary depending on the Sensor and Manager software versions you are using. Review this table to know the various combinations and what version you must enter to make sure you download the appropriate Gateway Anti-Malware Engine version.

<table>
<thead>
<tr>
<th>Manager</th>
<th>Sensor</th>
<th>What you must enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-8.2.7.83</td>
<td>Pre-8.2.5.145</td>
<td>8.2 and the build number.</td>
</tr>
<tr>
<td>8.2.7.83</td>
<td>8.3.5.145</td>
<td>8.2 and the build number.</td>
</tr>
<tr>
<td>8.3.7.83 or later</td>
<td>Pre-8.3.5.145</td>
<td>Manual import is not allowed. You must either upgrade the Sensor software version or assign the Sensor to a Pre-8.2.7.83 Manager.</td>
</tr>
</tbody>
</table>

NTBA does not allow manual update of Gateway Anti-Malware Engine.
5 Click Generate Update Package.

**Manual Update**

**Download Update Package for McAfee® Products**
If you have a valid licensed McAfee product you can manually download personalized update packages. These update packages can be used for a manual import into your McAfee product. Please finish the following steps to start the generation of your personalized update package.

**Step 4/4**
Please select updates to include in the update package
- McAfee Gateway Antimalware (~110+ MB)

[Cancel] [Previous Step] [Generate Update Package]

After the package is generated, you are shown details about the file such as file-size and MD5 checksum.

6 Click Download and save the package to a convenient location.

**Manual Update**

**Download Update Package**
Your personalized update package is valid for the following product:
- McAfee Network Security Appliance Version 8.2 Build 8.2.5
- Linux (x86_64)
- Included Updates
  - McAfee Gateway Antimalware

[Cancel] [Previous Step] [Download]

7 After the file is downloaded, log on to the Manager and go to Manage | Updating | Manual Import.

8 In the Manual Import page, click Choose File and navigate to the file location to select it.

9 Select the file and click Import.

  A pop-up opens giving you the status of the upload.

10 After the upload is complete, go to Devices | <Admin Domain Name> | Devices | <Device Name> | Deploy Pending Changes.

  The Pending Changes column displays New Gateway Anti-Malware Versions.

11 Select the checkbox for GAM Updates and click Update.

  A pop-up window appears showing you the status of the update. If the update fails, it is likely that you might have downloaded an incompatible version. Review the compatible versions and the
combinations, listed in step 4 of this section, to ascertain if you have downloaded the appropriate version.

**Manage failover pairs**

When you go to Devices | <Admin Domain Name> | Global | Failover Pairs, you can add new failover pairs. A failover pair will be managed just as any other device is managed, by going to Devices | <Admin Domain Name> | <Device Name> | Devices

Using the Failover Pairs tab, you can enable failover configuration for two identical Network Security Sensor models. The term "failover pair" refers to the pair of devices that constitute the Primary-Secondary arrangement required for failover functionality. The Primary/Secondary designation is used purely for configuration purposes and has no bearing on which device considers itself active. Primary device designation determines which device's configuration is preserved and copied to the Secondary device by Manager. Both devices receive configuration and update changes from Manager; however, the Secondary accepts the changes as if they are coming directly from the Primary device. In the event of primary failure, the Secondary device will see all changes as coming directly from Manager.

Two devices in a failover pair can have different fail-open/fail-closed settings. It is possible to configure, for example, one device to fail open, and the second device to fail closed. The intended use of this option is in an Active-Standby configuration with the Active link configured to fail closed (to force traffic to the standby link in case of failure), and the Standby link configured to fail open (to provide uninterrupted traffic flow should both devices fail).

For more information on high availability using failover pairing, see the *McAfee Network Security Platform IPS Administration Guide*.

<table>
<thead>
<tr>
<th>I-series Sensor model</th>
<th>Port(s) used for failover</th>
</tr>
</thead>
<tbody>
<tr>
<td>I-4010</td>
<td>6A and 6B</td>
</tr>
<tr>
<td>I-4000</td>
<td>2A and 2B</td>
</tr>
<tr>
<td>I-3000</td>
<td>6A and 6B</td>
</tr>
<tr>
<td>I-2700</td>
<td>4A. Note that 4B remains unused.</td>
</tr>
<tr>
<td>I-1400</td>
<td>Response Port (R1)</td>
</tr>
<tr>
<td>I-1200</td>
<td>Response Port (R1)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>M-series Sensor model</th>
<th>Port(s) used for failover</th>
</tr>
</thead>
<tbody>
<tr>
<td>M-8000</td>
<td>3A and 3B</td>
</tr>
<tr>
<td>M-6050</td>
<td>4A. Note that 4B remains unused.</td>
</tr>
<tr>
<td>M-4050</td>
<td>2A</td>
</tr>
<tr>
<td>M-3050</td>
<td>2A</td>
</tr>
<tr>
<td>M-2950</td>
<td>6A</td>
</tr>
<tr>
<td>M-2850</td>
<td>6A</td>
</tr>
<tr>
<td>M-1450</td>
<td>4A</td>
</tr>
<tr>
<td>M-1250</td>
<td>4A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NS-series Sensor model</th>
<th>Port(s) used for failover</th>
</tr>
</thead>
<tbody>
<tr>
<td>NS9100</td>
<td>G0/1</td>
</tr>
<tr>
<td>NS9200</td>
<td>G0/1</td>
</tr>
<tr>
<td>NS9300</td>
<td>G1/1 and G1/2 (40G QSFP+)</td>
</tr>
</tbody>
</table>
To configure two devices for failover, do the following:

**Task**

2. Click New. The Add a Failover Pair dialog opens.

   ![Add a Failover Pair window](figure)

   The **Add** button shows up in the UI only when there are at least two devices of the same model in the Device List node and a failover pair has not been created using these two devices.

3. Select the **Model**. Both devices in a failover pair must be the same model.
4. Type a failover pair **Name** that will uniquely identify the grouping.
5. Select the **Template Device** from the drop-down menu.
6. Select the **Peer Device** from the drop-down menu.
7. Enable or disable **Fail open** for the failover pair as per your requirement. By default, it is disabled.
8. Click **Create**; click **Cancel** to abort. Upon saving, a message informs you that the failover pair creation will take a few moments. Click **OK**. The new failover pair will appear as a child node of the devices node under which it was created.

   If you have created a failover pair while maintaining an open Threat Analyzer window, the Threat Analyzer will continue to report alerts from both the Primary and Secondary devices, respectively, identifying each device by the given device name and not by the name of the failover pair. This may cause confusion in the event that both devices detect identical alerts. (In true failover operation, if both devices detect the same alert, only one alert instance is reported with the name of the failover pair as the identifying device.) Restart the Threat Analyzer for proper alert reporting. The same is true in reverse if a failover pair is deleted. You must restart the Threat Analyzer to view alerts separately from each device.

**Tasks**

- Changing reserved VLAN ID within a failover pair on page 97
Changing reserved VLAN ID within a failover pair

In cases where the reserved device VLAN ID conflicts with one already used on your network, change the reserved VLAN ID.

The Device Reserved VLAN ID field is displayed only for I-3000 and I-4010 models.

To change the reserved VLAN ID for a Failover Pair:

**Task**

1. Select the Manage Cluster Configuration tab for the failover pair interface. (Failover-Pair-Name | Physical Failover Pair | Cluster Settings)
2. Type a new Device Reserved VLAN ID.
3. Click Submit.

Specify proxy server for internet connectivity

If you employ a proxy server for internet connectivity, you can configure the Manager or your devices to connect to that server for proxy service. This is necessary if you want to download updates directly to Manager from the update server or if you wish to download host reputation and country of origin information during integration with McAfee® TrustedSource™.

The Manager supports application-level HTTP/HTTPS proxies, such as Squid, iPlanet, Microsoft Proxy Server, and Microsoft ISA.

To use Microsoft ISA, you must configure this proxy server with basic authentication. Network Security Platform does not support Microsoft ISA during NTLM (Microsoft LAN Manager) authentication.

SOCKS, a network-level proxy, is not currently supported by Network Security Platform.

Follow this procedure to specify your proxy server:

**Task**

1. Select Manage | <Admin Domain> | Setup | Proxy Server.
   - The Proxy Server page is displayed.
2. Select the Use a Proxy Server? checkbox.
3. Enter the Proxy Server Name or IP Address. This can be either IPv4 or IPv6 address.
4. Enter the Proxy Port of your proxy server.
5. Enter Username and Password.
6. Provide the appropriate URL. You may test to ensure that the connection works by entering a Test URL and clicking Test Connection.
7. Click Save to save your settings.
   - When the Manager or the device makes a successful connection, it displays a message indicating that the proxy server settings are valid.
Configure NTP server

NTP support allows you to configure the Sensor as an NTP client that synchronizes time from a public NTP server instead of updating time only with the Manager server.

If NTP is configured and Manager connectivity is established, then the Sensor receives time from both the NTP server and the Manager. If there is loss of connectivity with either the Manager or NTP server, then the other takes over as the time source.

The Manager should be synced with an NTP server, prior to starting NTP on the Sensor. Not doing this will break the communication between the Sensors and the Manager.

If the Manager is not using the time received from the NTP server then while switching from NTP server to the Manager and vice versa, there might be issues because of the time difference.

To specify your NTP server, do the following:

**Task**

1. Select Devices | ‹Admin Domain Name› | Global | Default Device Settings | Common | NTP.

   The NTP Server page appears.

   The NTP can also be configured for each device as well.

2. To enable communication with the NTP server, select Enable NTP Server?

   To stop NTP from the Manager, unselect this option.

3. Configure the two NTP servers: the Sensor will use one of the configured NTP servers based on least RTT (Round-Trip Time).
   a. Type the IP Address. This can be an IPv4 or IPv6 address.
   b. Enter the Polling Interval. The range is 3 ~ 17. The configured polling interval is applied as 2^x seconds (2 power x).
   c. Select Authentication to enable authenticating the NTP servers.
   d. Enter the Authentication Key and Authentication Key ID.
   e. Select the Authentication Key Type; MD5, SHA, or SHA1.

   The parameters in d and e are provided by the NTP service provider.
f Click on the Test Connection button to check the connectivity to the NTP server. The status of the connectivity tests is displayed in the NTP page.

g Click Save to save your settings.

The IPv4 and IPv6 addresses are mutually exclusive. At any configuration either the IPV4 or IPV6 address will be used. For the IPV6 address to work, the Sensor management port should be assigned an IPV6 address.

Figure 6-23 Configure NTP servers

Configure NTP server for a device

NTP support allows you to configure the Sensor as an NTP client that synchronizes time from a public NTP server instead of updating time only with the Manager server.

If NTP is configured and Manager connectivity is established, then the Sensor receives time from both the NTP server and the Manager. If there is loss of connectivity with either the Manager or NTP server, then the other takes over as the time source.

The Manager should be synced with an NTP server, prior to starting NTP on the Sensor. Not doing this will break the communication between the Sensors and the Manager.

If the Manager is not using the time received from the NTP server then while switching from NTP server to the Manager and vice versa, there might be issues because of the time difference.

To specify your NTP server, do the following:

**Task**

1. Select Devices | Admin Domain Name | Devices | Device Name | Setup | NTP.

   The NTP Server page appears.

   The NTP can also be configured for each device as well.

2. Deselect Inherit Settings? to override the configuration in the parent domain.
To enable communication with the NTP server, select **Enable NTP Server**?
To stop NTP from the Manager, unselect this option.

Configure the two NTP servers: the Sensor will use one of the configured NTP servers based on least RTT (Round-Trip Time).

- **a** Globalyype the **IP Address**. This can be an IPv4 or IPv6 address.
- **b** Enter the **Polling Interval**. The range is $3 \sim 17$. The configured polling interval is applied as $2^x$ seconds ($2$ power $x$).
- **c** Select **Authentication** to enable authenticating the NTP servers.
- **d** Enter the **Authentication Key** and **Authentication Key ID**.
- **e** Select the **Authentication Key Type**; MD5, SHA, or SHA1.

> The parameters in steps d and e are provided by the NTP service provider.

- **f** Click on the **Test Connection** button to check the connectivity to the NTP server. The status of the connectivity tests is displayed in the NTP page.
- **g** Click **Save** to save your settings.

The IPv4 and IPv6 addresses are mutually exclusive. At any configuration either the IPv4 or IPv6 address will be used. For the IPv6 address to work, the Sensor management port should be assigned an IPv6 address.

### NTP Servers Configuration

<table>
<thead>
<tr>
<th>NTP Server 1</th>
<th>NTP Server 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address:</td>
<td>IP Address:</td>
</tr>
<tr>
<td>Polling Interval:</td>
<td>Polling Interval:</td>
</tr>
<tr>
<td>Authentication Key ID:</td>
<td>Authentication Key ID:</td>
</tr>
<tr>
<td>Authentication Key Type:</td>
<td>Authentication Key Type:</td>
</tr>
</tbody>
</table>

**Figure 6-24 Configure NTP servers**
Managing configuration for each device

The Devices tab in the Devices page represents the physical Sensor installed in your network. Each device is a uniquely named (by you) instance of a Sensor. All actions available in the <Device_Name> page customize the settings for a specific Sensor.

After properly installing and initializing a Sensor, then adding the Sensor to the Manager, it appears in the Device drop down list, where it was added, and inherits all of the configured device settings. After adding a device, the device can be specifically configured to meet user requirements by selecting the uniquely named device node.

For more information on interfaces and subinterfaces, see Network Security Platform IPS Administration Guide.

Many device configurations performed within the Devices page do not immediately update to the devices. You must perform either update the configuration of all devices or the specific device to push the configuration information from Manager to your device.

The <Device_Name> page for a Sensor in general contains Summary, Policy, Setup, Maintenance, Troubleshooting, Deploy Configuration Changes, and IPS Interfaces pages.

Contents

- Configuration and management of devices
- Troubleshooting your device configuration
- Management of device access

Configuration and management of devices

The <Device_Name> once selected from the drop down sets specific rules for the chosen device. The available actions are as follows:

- Viewing the details of a selected Device— View/edit a device details.
- Configuring device monitoring and response ports— View/edit the parameters of ports on a specific device.
- Updating the software on a Device— Update the software on a device.
- Rebooting a Device— Reboot a device.
- Shutting down a Device— Shut down (turns off) a device.
Update configuration of a Sensor or an NTBA Appliance

Configuration updates refer to changes to device and interface/subinterface configurations, such as port configuration, non-standard ports, interface traffic types, and configuration changes to the Sensor or NTBA Appliance.

Signature updates have new and modified signatures that can apply to the attacks enforced in a chosen policy. Policy changes update the device in case of a newly applied policy or changes made to the current enforced policy.

You can schedule configurations to be pushed to the NTBA Appliances and Sensors from Manage | <Admin Domain Name> | Automatic Updating | IPS Signature Sets. The Automatic IPS Signature Set Deployment options allow you to set the time when these configurations can be deployed on Sensors and NTBA. Configurations are automatically deployed based on schedule.

All configurations in the Policy page that apply to your Sensors or NTBA Appliance can also be manually pushed from Devices | <Admin Domain Name> | Global | Deploy Pending Changes (all Sensors and NTBA Appliances in a domain) or Devices | <Admin Domain Name> | Devices | <NTBA Appliance> | Deploy Pending Changes (to a single Sensor or NTBA Appliance) action.

Scheduled deployment

1. Select Manage | <Admin Domain Name> | Automatic Updating | IPS Signature Sets. The IPS Signature Sets page is displayed.

![Figure 7-1 IPS Signature Sets page](image)

2. From the Automatic IPS Signature Set Deployment options set the schedule for deploying signature updates:
   - For Deploy in Real Time, select Yes. (This option pushes signature sets update to all Sensors and NTBA Appliances immediately after it is downloaded to the Manager.) By default, No is the default option.
   - For Deploy at Scheduled Interval, select Yes to schedule for automatic deployment of signature sets.
   - In Schedule, set the frequency by which you want the Manager to check for a newly downloaded signature set. The choices are:
     - Frequently — Several times a day during a specified period at interval indicated in the Recur every option
     - Daily — Once a day
     - Weekly — Once a week
   - Select the Start Time, End Time, and Recur every options to specify intervals. Based on Schedule frequency, these fields allow you to select options.

3. Click Save.

On-demand deployment
Task

1. Select Devices | <Admin Domain Name> | Devices | <NTBA Appliance> | Deploy Pending Changes.

The Deploy Pending Changes page is displayed.

![Figure 7-2 Deploy Pending Changes page](image)

2. View the update information. If changes have been made, the Configuration & Signature Set column is checked by default.

3. Click Update.

A pop-up window displays configuration download status.

Update software for a Sensor or NTBA Appliance

The Upgrade action enables an on-demand download of the latest or earlier software updates for a Sensor or NTBA Appliance from your Manager. All the software versions, applicable to the device and available in the Manager are listed. From this, you can choose the version that you want to push to the device. These versions are the ones that you downloaded from the update server onto your Manager.

You can only update online devices. Make sure it is discovered, initialized, and connected to the Manager.

You can switch between different minor versions of the device software. Consider the scenario where you downloaded 6.0.1.1, 6.0.1.2, and 6.0.1.3 versions for M6050 Sensors from the update server onto the Manager. Also, assume that currently the M6050 Sensor that you want to update is on 6.0.1.2. You can now update this Sensor to either 6.0.1.1 or 6.0.1.3. Subsequently, you can also revert to 6.0.1.2. However, you cannot switch between major versions of the software through the Manager. For example, you cannot switch between 6.0 and 5.1 versions of device software using the Manager.

After you update the software of a device, you must restart it.

Task

1. Click Devices | <Admin Domain Name> | Devices | <Device Name> | Maintenance | Deploy Device Software.

The Deploy Device Software page is displayed.

In case of Sensors in fail-over pair, select a Sensor under the fail-over pair name node, and then select Upgrade.

<Device_Name> refers to name of the Sensor or NTBA Appliance.

2. Select the required version from the Software Ready for Installation section.

The Software Ready for Installation section lists the applicable versions of software that you downloaded from the update server (Manage | Updating | Download Device Software).

3. Click Upgrade.

When a device is being updated, it continues to function using the software that was present earlier.
4. After the update is complete, restart the Sensor or NTBA Appliance.

If the device that you updated is a Sensor in a fail-over pair (not applicable to NTBA Appliance), then update the other Sensor in the pair also to the same version. Note that both the Sensors of a fail-over pair need to be of the same software version.

**Shut down a Sensor or NTBA Appliance**
The **Shut Down** action turns off a Sensor or an NTBA Appliance with no restart.

**Task**
1. Select Devices | <Admin Domain Name> | Devices | <Device Name> | Maintenance | Shut Down.

   The **Shut Down** page is displayed.

2. Click **Shut Down Now**.

   The **<Device Name>** could be a Sensor or an NTBA Appliance.

**Troubleshooting your device configuration**

Using the **Troubleshooting** tab, you can perform the following actions:

- Upload a diagnostic trace
- Enable layer 2 settings

**Upload diagnostics trace**
The **Diagnostics Trace** action uploads a device diagnostics log from a Sensor or NTBA Appliance to your Manager server. The diagnostics file includes debug, log, and other information that can be used to determine device or NTBA Appliance malfunctions or other performance issues. Once uploaded to your Manager, this file can be sent through email to McAfee Technical Support for analysis and troubleshooting advice.

**Task**
1. Select Devices | <Admin Domain Name> | Devices | <Device Name> | Troubleshooting | Diagnostics Trace.

   The **<Device Name>** could refer to a Sensor or an NTBA Appliance.

   The **Diagnostics Trace** page is displayed.

   ![Diagnostics Trace page](image)

2. Select the **Upload?** checkbox if it is not already selected.
3 Click Upload.
The status appears in the Upload diagnostics Status pop-up window.

4 Click Close Window when the message "DOWNLOAD COMPLETE" appears. The trace file is saved to your Manager server at:
<Install Dir> \temp \tftpin \< Device Name \trace\. Once downloaded, the file also appears in the Uploaded Diagnostics Trace Files dialog box under this action.

5 [Optional] Export a diagnostics file to a client machine by selecting the file from the Uploaded Diagnostics Files listed and clicking Export. Save this file to your client machine. Saving the file is particularly useful if you are logged in remotely, need to perform a diagnostics trace, and send the file to technical support.

Management of device access

From the device Access tab, you can perform the following actions:

- Configure TACACS+ authentication
- Configure NMS objects

Configure TACACS+ authentication

The TACACS+ action enables you to enable and disable TACACS+ authentication for the selected device.

Task
1 Select Devices | <Admin Domain Name> | Devices | <Device_Name> | Setup | Remote Access | TACACS+.

2 Select Yes to enable TACACS+.

3 Select Inherit from Parent Domain to use the TACACS+ settings in the parent domain.

4 Enter the TACACS+ Server IP Address in the IP Address fields; you can enter up to four IP Addresses for the TACACS+ server. At least one IP Address is required if you enable TACACS+.

5 Select Yes to Enable Encryption.
When you enable encryption, you need to enter an encryption key in the Enable Encryption field. The maximum length of the key is 64 bytes.

6 Click Save to save the configuration.

Configuration of NMS objects

You can configure the device to provide configuration information and statistics to a Network Management System (NMS) via SNMPv3.
From the NMS menu, you can perform the following actions:

- Manage NMS users
- Manage NMS IPs

**Management of NMS users**

The NMS Users tab enables you to manage NMS users at the device level.

The device has to be in the active state to manage NMS users. The device can create its own NMS users or can associate users from the domain. Only 10 users can be configured in the device.

During export and import of device configuration, only the users created in the device directly are considered, the users allocated from the domain are not considered.

The NMS users function allows you to do the following:

- Allocating users from domain—Add available users from domain to the device.
- Adding new NMS users to the Device—Add new users to the device.
- Editing a NMS User—Edit the NMS users.
- Deleting an NMS User—Delete allocated NMS users from device or delete new users from devices.

### Assign an NMS user

To assign a previously existing NMS user, do the following:

**Task**


2. Click Assign Domain User.

   - The user list includes all the users defined in the domain in which the device is being added and its parent domain users.

3. Select the NMS user from the list.

4. Click Assign; click Cancel to abort.

### Add a new NMS users

NMS users can be added from the device and from the domain.
**Task**

1. To add a new NMS user:
   - From the Global tab, select Devices | <Admin Domain Name> | Global | Common Device Settings | Remote Access | NMS | NMS Users.
   - From the Device tab, select Devices | <Admin Domain Name> | Devices | <Device_Name> | Setup | Remote Access | NMS | NMS Users.

2. Click New.

   ![Figure 7-5  Add NMS User Account dialog](image)

   The Add NMS User Account dialog is displayed.

3. Enter the User Name.
   - The length of the user name should be between 8 to 31 characters. It can consist of alphabets and numerals. Special characters and spaces are not allowed.

4. Enter the Authentication Key (re-enter at Confirm Authentication Key).

5. Enter the Private Key (re-enter at Confirm Private Key).
   - The length of the Authentication and Private key should be between 8 to 15 characters.
   - Since the communication is over SNMP version 3, the supported authentication protocol is "MD5" and encryption algorithm is "DES".

6. Click Save.
   - The user is now added to the device and is displayed in the NMS User table.

**Edit an NMS user**

NMS users can be edited from the device and from the domain.

**Task**

1. To edit an existing NMS user:
   - From the Global tab, select Devices | <Admin Domain Name> | Global | Common Device Settings | Remote Access | NMS | NMS Users.
   - From the Device tab, select Devices | <Admin Domain Name> | Devices | <Device_Name> | Setup | Remote Access | NMS | NMS Users.
   - Users created only at the device level are editable from the Device Settings tab of the specific device.

2. Select the NMS user created in the device from the list.

3. Click Edit.
4 Enter the Authentication Key and Private Key (confirm at Confirm Authentication Key and Private Key).

5 Click Save; click Cancel to abort.

**Delete an NMS user**

NMS users can be deleted from the device and from the domain.

**Task**

1 To delete an NMS user:
   - From the Global tab, select Devices | <Admin Domain Name> | Global | Common Device Settings | Remote Access | NMS | NMS Users.
   - From the Device tab, select Devices | <Admin Domain Name> | Devices | <Device_Name> | Setup | Remote Access | NMS | NMS Users.

2 Select the user from the NMS User List.

3 Click Delete.

4 Confirm deletion by clicking OK.

**Management of NMS IP addresses**

The NMS IP action allows you to do the following:

- Allocating IP addresses from domain—Add IP addresses to device.
- Adding new NMS IP address to the device—Allocate available IP addresses from the domain.
- Deleting NMS IP addresses—Delete NMS IP addresses from device and domain.

Third-party NMS (SNMP over IPv6) is supported only on 8500 ports of I-series Sensors. NMS will not work for default port 161 of I-series, M-series and NS-series Sensors.

**Allocate an IP addresses**

The device can inherit NMS IP address configuration from domain. To allocate an IP address, do the following:

**Task**

1 Select Devices | <Admin Domain Name> | Devices | <Device_Name> | Setup | Remote Access | NMS | NMS Devices

2 Click Assign Domain IP.

3 Select the NMS IP address.

4 Click Assign; click Cancel to abort.

**Add a new NMS IP address**

NMS IP addresses can be added from the device and from the domain.
Task
1 To add a new NMS IP address:
   • From the Global tab, select Devices | <Admin Domain Name> | Global | Common Device Settings | Remote Access | NMS | NMS Devices.
   • From the Device tab, select Devices | <Admin Domain Name> | Devices | <Device_Name> | Setup | Remote Access | NMS | NMS Devices.

2 Click New.

Figure 7-6 Add NMS IP dialog
The Add NMS IP page is displayed.

3 In IP Address, enter the NMS IP address. You can enter either IPv4 or IPv6 address.

   While adding NMS IP address, you can add a maximum of 10 IPv4 addresses and 10 IPv6 addresses.

4 Click Save.

Delete NMS IP addresses
NMS IP addresses can be deleted from the device and from the domain.

Task
1 To delete an NMS IP address:
   • From the Global tab, select Devices | <Admin Domain Name> | Global | Common Device Settings | Remote Access | NMS | NMS Devices.
   • From the Device tab, select Devices | <Admin Domain Name> | Devices | <Device_Name> | Setup | Remote Access | NMS | NMS Devices.

2 Select the IP address from the Permitted List.

3 Click Delete.

4 Confirm deletion by clicking OK.

If allocated IP addresses are deleted, then it is deleted only from the device and not from the domain.

Users can communicate to the device from only the NMS IP addresses added above. User may be able to communicate with the device until 180 inactive seconds from the deleted IP address, if a request is made from the same IP address before 180 seconds, then the connection from that IP address is still valid for another 180 seconds.
Configuration of the Update Server

After installing the Manager software, one of the first tasks you will perform is setting the schedule for receiving updates from the McAfee® Network Security Update Server (Update Server). These updates include signature files for your Sensors and software for your Manager and/or Sensors.

You can only perform one download/upload at a time from any Network Security Platform component, including the Update Server.

You can perform the following actions using the Update Server:

- Downloading software updates— Download the latest Sensor or NTBA Appliance software image file from the Update Server to the Manager.
- Downloading signature set updates— Download the latest attack and signature information from the Update Server to the Manager.
- Automating updates— Configure the frequency by which the Manager checks the Update Server for updates, and the frequency by which Sensors and NTBA Appliances receive signature updates from the Manager.
- Manually importing a Sensor and NTBA Appliance image or signature set— Manually import downloaded Sensor or NTBA Appliance software image and signature files to the Manager.

For more information on the Update Server, see *McAfee Network Security Platform Manager Administration Guide*. 
Uninstallation of the Manager/Central Manager

You uninstall McAfee® Network Security Manager (Manager) and McAfee® Network Security Central Manager (Central Manager) using the standard Windows Add/Remove Programs feature.

Contents

- Uninstall using the Add/Remove program
- Uninstall using the script

Uninstall using the Add/Remove program

You must have Administrator privileges on your Windows server to uninstall McAfee Network Security Manager (Manager) or McAfee Network Security Central Manager (Central Manager). Follow the steps given below for uninstalling Central Manager and Manager.

To uninstall the Manager software:

McAfee recommends you stop the Manager service and applicable Java services before starting an uninstall. If not, you will have to manually delete files from the Network Security Platform program folder.
Task

Figure 9-1 Uninstall Manager window
2 Click **Uninstall** to start the uninstallation process.

3 After uninstallation, the message **All items were successfully uninstalled** is displayed.

![Uninstall Complete window](image)

**Figure 9-2 Uninstall Complete window**

Uninstallation of the Network Security Platform database (MySQL) is not part of this uninstallation.

---

**Uninstall using the script**

You can also uninstall the McAfee Network Security Manager (Manager)/McAfee Network Security Central Manager (Central Manager) by executing a script from the Network Security Platform program folder.

To uninstall via script:

**Task**

1 Navigate to the directory containing the uninstallation script. The default path is: `<Network Security Platform installation directory>\UninstallerData`

2 Run

   `Uninstall ems.exe`
Uninstallation of the Manager/Central Manager
Uninstall using the script
Upgrading Network Security Platform

Chapter 10  Overview
Chapter 11  Management of a heterogeneous environment
Chapter 12  How to upgrade the Central Manager?
Chapter 13  How to Upgrade the Manager?
Chapter 14  How to perform signature set and Sensor software upgrade
Chapter 15  Upgrade information for NTBA and XC Cluster
Chapter 16  Uninstalling the upgrade
Overview

This guide primarily provides information on how to upgrade your McAfee® Network Security Platform setup to the latest 8.2 release from the following versions:

- 7.1
- 7.5
- 8.1
- Initial 8.2 versions

Important Notes:

- If you have any M-series Sensors on 6.1 software, you can directly upgrade those Sensors from 6.1 to 8.1. However, before you upgrade the 6.1 M-series Sensors to 8.1, you must first upgrade the Manager to 8.1. For related information, refer to McAfee Network Security Platform 8.1 Upgrade Guide. When both the Manager and the M-series Sensors are on a required version of 8.1, you can begin the 8.2 upgrade process.

- In case of Network Security Platform 8.0, first upgrade to a supported version of 8.1 or 8.2 to upgrade to the latest version of 8.2.

- The Network Security Platform 8.2 release is specific to the Central Manager, Manager, M-series Sensors, NS-series Sensors, Virtual IPS Sensors, Network Threat Behavior Analysis (NTBA) devices, and XC Cluster devices.

- As with any upgrade, McAfee strongly recommends that you always first try the upgrade on a test environment.

- The current version of 8.2 Manager software can be used to configure and manage the following appliances:
  - M-series Sensors on 7.1, 7.5, 8.0, 8.1, and 8.2 software.
  - Virtual IPS Sensors on 8.0, 8.1, and 8.2 software.
  - NS-series Sensors on 7.1, 8.0, 8.1, and 8.2 software.
  - I-series Sensors 7.1 software.
  - XC Cluster appliances on 7.1, 7.5, 8.0, 8.1, and 8.2 software.
  - NTBA appliances (physical and virtual) on 7.1, 7.5, 8.0, 8.1, and 8.2 software.
  - Virtual Security System appliances on 8.1.

- The upgrade involves the following phases that you must complete in the same order:
  1. If applicable, McAfee® Network Security Central Manager upgrade.
3 McAfee® Network Security M-series, NS-series Sensor, or Virtual IPS Sensor software upgrade.

4 If applicable, XC-240 Load Balancer and M-8000XC Sensor upgrade.

5 If applicable, NTBA appliance upgrade.

• **Removal of Network Access Control (NAC):**
  From 8.1, Network Security Platform no longer supports the Network Access Control module. If you are using Network Access Control with N-series (NAC-only) Sensors, McAfee recommends that you continue to use the 6.x version. If you are using the Network Access Control module in M-series Sensors, continue to use the 7.x version. That is, you should not upgrade the Manager or the Sensors for such cases.

• No software is released for I-series and N-series (NAC-only) Sensors as part of Network Security Platform 8.2.

You need the following documents during the upgrade process:

* McAfee Network Security Platform 8.2 Manager Administration Guide
* McAfee Network Security Platform 8.2 IPS Administration Guide
* McAfee Network Security Platform 8.2 CLI Guide
* McAfee Network Security Platform 8.2 NTBA Administration Guide
* McAfee Network Security Platform 8.2 Troubleshooting Guide

**Contents**

- Important requirements and considerations
- Migration from 1024-bit to 2048-bit encryption

**Important requirements and considerations**

Review these important requirements carefully before you proceed with the upgrade.

• This document provides information on how to upgrade from Network Security Platform 7.1, 7.5, or 8.1 version to 8.2 version. See the corresponding upgrade guide and release notes to first upgrade to the minimum required version for 8.2. Consider that your current version is in the 7.1 release train but your current version is not supported for upgrade to 8.2. Then, see the latest Network Security Platform 7.1 Upgrade Guide and upgrade to the latest 7.1 version before you upgrade to 8.2.

• The minimum required software versions to upgrade to 8.2 are provided in the following sections:
  - Minimum required Manager version.
  - Sensor upgrade requirements on page 189.
  - Upgrade information for NTBA and XC Cluster on page 5.

• After you upgrade the Central Manager or the Manager to 8.2, you might be prompted to restart the server. If prompted, it is highly recommended that you restart the server.
Currently port 4167 is used as the UDP source port number for the SNMP command channel communication between Manager and Sensors. This is to prevent opening up all UDP ports for inbound connectivity from SNMP ports on the sensor. Older JRE versions allowed the Manager to bind to the same source port 4167 for both IPv4 and IPv6 communication. But from JRE version 1.7.0_45, it is no longer possible to do so, and the Manager uses port 4166 as the UDP source port to bind for IPv6.

The latest 8.2 Manager server uses JRE version 1.7.0_76. If you have IPv6 Sensors behind a firewall, you must update your firewall rules accordingly such that port 4166 is open for the SNMP command channel to function between those IPv6 Sensors and the Manager. This applies to a local firewall running on the Manager server as well. You must complete updating your firewall rules before you begin the 8.2 upgrade.

The following are the additional ports that are used for Sensor-to-Manager communication in release 8.2. Before you begin the 8.2 upgrade process, make sure that your firewall rules are updated accordingly to open up the required ports. This applies to a firewall that resides between the Sensor and the Manager (including a local firewall on the Manager server).

<table>
<thead>
<tr>
<th>Port #</th>
<th>Protocol</th>
<th>Description</th>
<th>Direction of communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>8506</td>
<td>TCP</td>
<td>Proprietary ((install channel for 2048-bit certificates). For information on 2048-bit certificates, see Migration from 1024-bit to 2048-bit encryption on page 121</td>
<td>Sensor--&gt;Manager</td>
</tr>
<tr>
<td>8507</td>
<td>TCP</td>
<td>Proprietary (alert channel/control channel for 2048-bit certificates).</td>
<td>Sensor--&gt;Manager</td>
</tr>
<tr>
<td>8508</td>
<td>TCP</td>
<td>Proprietary (packet log channel for 2048-bit certificates).</td>
<td>Sensor--&gt;Manager</td>
</tr>
<tr>
<td>8509</td>
<td>TCP</td>
<td>Proprietary (Bulk file transfer channel for 2048-bit certificates).</td>
<td>Sensor--&gt;Manager</td>
</tr>
<tr>
<td>8510</td>
<td>TCP</td>
<td>Proprietary (Bulk file transfer channel for 1024-bit certificates).</td>
<td>Sensor--&gt;Manager</td>
</tr>
</tbody>
</table>

Migration from 1024-bit to 2048-bit encryption

Sensor-Manager communication happens over both 1024-bit and 2048-bit channels. This two-channel set option allows heterogeneous deployments currently using 1024-bit encryption to communicate with later versions that use 2048-bit encryption.

The Manager and Sensor establish trust using 2048-bit encryption keys for Network Security Platform 8.1 or later. To make sure that migration is seamless for existing deployments that might be heterogeneous or homogeneous environments, your role in the migration is minimal. To learn about heterogeneous environments, refer to Managing a Heterogeneous Environment

Heterogeneous deployments currently on earlier versions such as 7.x Sensor, which only support 1024-bit encryption are capable of coexisting with 8.1 or later software which supports 2048-bit encryption.
The general sequence of an upgrade follows this sequence:

1. The ports necessary for 2048-bit encryption are confirmed as opened.
2. The Manager is upgraded to a version that supports 2048-bit encryption. After the upgrade is complete, the Sensors continue to connect to the Manager by establishing trust using 1024-bit encryption.
3. One of the Sensors is upgraded to a version that supports 2048-bit encryption. After the upgrade is complete, the Sensors continue to connect using 1024-bit encryption. The Sensor that is upgraded then initiates and upgrades its certificates, and attempts to connect to ports assigned for 2048-bit encryption in the Manager. After the certificates are updated, the Sensor and Manager can communicate using 2048-bit certificates.

### Upgrade to 2048-bit encryption

#### Before you begin

- Make sure you have a Sensor and Manager that are able to communicate with each other. They need not have established trust, but must be able to do so.
- Keep all essential ports open if you are using a firewall in your network. The following table shows you the ports used to establish trust using 2048-bit certificates.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8506</td>
<td>Install channel (TCP)</td>
</tr>
<tr>
<td>8507</td>
<td>Alert channel (TCP)</td>
</tr>
<tr>
<td>8508</td>
<td>Packet log channel (TCP)</td>
</tr>
</tbody>
</table>

- If SSL decryption is enabled, the Sensor will continue to connect using 1024-bit certificates and will not be able to transition to 2048-bit certificates. This happens because certificates stored in the Sensor are, at present, 1024-bit encrypted and is not in a position to accept those that are 2048-bit encrypted. Therefore, to make sure that 2048-bit encryption is eventually successful with SSL decryption, you must perform the following steps:
  1. Uninstall and reinstall the Sensor. This restores the Sensor to default settings in which SSL decryption is disabled.
  OR

  2. Disable SSL decryption in the Manager.
  3. Complete the upgrade to 2048-bit encryption.

The following steps will explain the procedure to upgrade to 2048-bit certificates.

#### Task

1. Upgrade the Manager to a version that supports 2048-bit encryption.

   You need to make sure that your current deployment supports this upgrade. For details on upgrading the Manager, refer to Upgrade requirements for the Manager on page 147.

   Once the Manager is upgraded, it continues to connect to the Sensors using 1024-bit certificates.
2 Upgrade the Sensor software to a version that supports 2048-bit certificates.
   As with the Manager, you will need to make sure that your present deployment supports such an upgrade. For details on upgrading the Sensor, refer to Sensor upgrade requirements on page 189.

Once the Sensor has been upgraded, it continues to connect to the Manager using 1024-bit certificates. The Sensor then initiates the upgrade to 2048-bit certificates. The Sensor checks to make sure the specific ports on the Manager assigned for connection using 2048-bit certificates are reachable. If they are reachable, the upgrade is complete.

During this step, the Sensor and Manager may not be able to connect using 2048-bit certificates if the Manager is on a version that does not support it.

If you have upgraded Sensor software using the CLI command, loadimage, you will be notified that 2048-bit connection has failed. You will also be prompted to confirm whether you wish to proceed with existing 1024-bit certificates. If you do not wish to do this, you may type N to discontinue the process and debug the problem.

However, if you have upgraded Sensor software from the Manager (which does not support 2048-bit encryption), the Sensor will proceed to establish trust using 1024-bit certificates.

View encryption type

Before you begin
Since trust between the Sensor and Manager is encrypted, you will be able to view the level of encryption only after trust has been established.

To view the type of encryption used in establishing trust between the Sensor and Manager, you will need to access the Sensor command line interface (CLI). The Sensor and Manager establish trust using 2048-bit certificates ports separate from those used for 1024-bit encryption.

The steps that follow tell you how you can view the encryption type and ports in the CLI.

Task
1 Use a hyperterminal and enter the Sensor IP address to access its CLI.
2 Enter your credentials for the Sensor.
Once you are in the CLI, enter `status` to view the type of encryption used to establish trust between the Sensor and Manager.

```plaintext
intrushell@M2850-Lab> st

[Sensor]
System Initialized    : yes
System Health Status  : good
Layer 2 Status        : normal (IDS/IPS/MAC)
Installation Status   : complete
IPv6 Status           : Don't Parse and Allow Inline
Reboot Status         : Required (SSL Config Change)
Guest Portal Status   : up
Hitless Reboot        : Not-Available
Last Reboot reason    : reset config issued from CLI

[Signature Status]
Present               : yes
Version               : 8.6.28.4
Geo Location database : Present
DAT file              : Absent

[Manager Communications]
Trust Established     : yes (RSA 2048-bit)
Alert Channel         : up
Log Channel           : up
Authentication Channel: up
Last Error            : None
Alerts Sent           : 0
Logs Sent             : 0

[Alerts Detected]
Signature             : 0       Alerts Suppressed : 0
Scan                   : 0       Denial of Service : 0
Malware                : 0
```

Figure 10-1  Trust established using 2048-bit certificates

The CLI displays **RSA 2048-bit** if the 2048-bit encryption was successful.
4 Enter `show` to bring up the ports used for 2048-bit encryption – 8506, 8507, and 8508.

```plaintext
[McAfee NTBA Communication]
Status: down
IP: 0.0.0.0
Port: 8505

[McAfee NATD Communication]
Status: down
IP: 0.0.0.0
Port: 8505

[McAfee NAC Communication]
Trust Status: No Trust
Root Certificate: None
intruShell@M2850-Lab> show
[Sensor Info]
System Name: M2850-Lab
Date: 3/17/2014 - 8:27:9 UTC
System Uptime: 13 days 03 hrs 30 min 50 secs
System Type: M-2850
Serial Number: S060211071
Software Version: 8.1.2.6
Upgrade/Downgrade Status: Upgrading to 8.1.2.6
Hardware Version: 1.00
MGMT Ethernet port: auto negotiated
MGMT port Link Status: link up
[Sensor Network Config]
IP Address: 10.213.174.202
Netmask: 255.255.255.0
Default Gateway: 10.213.174.252
Default TFTPserver: 10.213.173.1
SSH Remote Logins: enabled

[Manager Config]
Manager IP addr: 10.213.174.201 (primary intf)
Install TCP Port: 8506
Alert TCP Port: 8507
Logging TCP Port: 8508

[McAfee NAC Config]
McAfee NAC Server IP Address: 0.0.0.0
Console-to-Application Server Communication Port: 8443
Client-to-Server Authenticated Communication Port: 8444
McAfee NAC Server-to-Sensor Communication Port: 8445
Sensor-to-NAC Client Communication Port: 8444
```

*Figure 10-2* Ports used in 2048-bit encryption
Disable 2048-bit encryption

Before you begin
Before you begin, make sure to stop the Manager service.

If, at any point, you want to disable 2048-bit encryption in your deployment, you can do so by following these steps.

Task

1. Locate the `ems.properties` file in your Manager server. It is available by default at `C:\Program Files\McAfee\Network Security Manager\App\config`.

2. Open the file in a suitable text editor such as Windows Notepad.

3. Within the file search for the string, `iv.core.ControlChannel.is2048Enabled=`. In a default setup you will notice this to be set to `true`.

   ```
   # TEMPORARILY OVERRIDE THE PORTS BACK TO THE CURRENT VALUES TO GIVE
   # THE SENSOR TEAM TIME TO MIGRATE THEIR CODES.
   
   # Ports, ports, ...
   #iv.core.ControlChannel.installPort=8901
   #iv.core.ControlChannel.controlChannelPort=8902
   #iv.core.ControlChannel.packetLogPort=8503
   # Note, this is *NOT* really TFTP, it is the sensor download service
   #iv.core.tftpserver.tftpPort=8504
   #iv.core.ControlChannel.installPort2048=8506
   #iv.core.ControlChannel.controlChannelPort2048=8507
   #iv.core.ControlChannel.packetLogPort2048=8509
   ## # ACM server port
   ## #iv.core.service.port=8555
   ## # Raw Alert Channel port
   ## #iv.core.rawalert.port=8554
   
   ## #2048 Key Support
   iv.core.ControlChannel.is2048Enabled=false
   
   ## # alertcache
   ## # (small to start with)
   ## #iv.core.alert.cache.size=100000
   ## #iv.core.alert.cache.numBucket=10
   ## #load 10 days worth for now, given the state of testing data.
   ## #iv.core.alert.cache.oldAlarmInterval=364800
   ## # 0 means use the cache size
   ## #iv.core.alert.cache.oldAlarmCount=0
   ##
   
   Figure 10-3 Ems properties file shows 2048-bit encryption disabled
   ```

4. Change this value to `false`.

5. Remove hash (`#`) symbols that indicate this to be a comment.

6. Save the file before you close.

7. Reboot the Manager.

Once the Manager comes back up, all Sensors will disconnect from the manager and manual intervention of the user will be required to connect the Sensor again. For information about establishing trust with Manager, refer to Add a Sensor to the Manager on page 57.
Network Security Platform 8.2 enables you to manage a heterogeneous environment of Managers and Sensors. If you do not require to manage a heterogeneous environment, you can skip this chapter. To know more about heterogeneous environments, see What are heterogeneous environments? on page 127.

This note is applicable only if you have NTBA devices on 7.1 and 7.5 managed by a Manager on 8.2. For 7.1 NTBA, the minimum version required for a heterogeneous NTBA environment is 7.1.3.26. For 7.5 NTBA, the minimum version required for a heterogeneous NTBA environment is 7.5.3.35.

**Contents**
- What are heterogeneous environments?
- When would you need a heterogeneous environment?
- Upgrade scenarios for heterogeneous environments
- Enhanced Central Manager/Manager user interface
- Feature support in a heterogeneous environment
- Heterogeneous support for NTBA devices
- Heterogeneous environment for XC Cluster

## What are heterogeneous environments?

Typically, the Manager and the Sensors under it are of the same major version. The term major version refers to the first two digits of a release. For example, in the case of Manager 8.1.7.5, the major version is 8.1. For Manager 7.5.3.11, the major version is 7.5.

If the Manager and the Sensors are of the same major version, it is referred to as a homogeneous environment. In a heterogeneous environment, the Manager and the Sensors are of different successive major versions. This similarly applies to Central Manager and the Managers as well.

The terms heterogeneous and homogeneous environments are with respect to the software versions only and have no relevance to the device model numbers.
**Management of a heterogeneous environment**

**When would you need a heterogeneous environment?**

Support for managing a heterogeneous environment is typically for large deployments where upgrade of the Managers or the Sensors happens in phases. Consider a deployment of over a hundred Sensors that are on 8.1.x.x. As part of the upgrade process, you first upgrade the Manager as well as some of the Sensors to 8.2. However, during this upgrade window, you might need to manage the 8.1 Sensors as well as be able to view the alerts raised by them. For some Sensor models, 8.2 version software might not be available currently, and you need to manage such Sensors as well. These are possible with a Manager version that supports a heterogeneous Sensor environment.

McAfee strongly advises that you use the heterogeneous support feature only for the interim until you upgrade all your Managers and Sensors to the latest version. This enables you to make use of the latest features in Network Security Platform.

---

**Notes:**

- A Manager must always be of the same or higher version than the corresponding Sensors. Therefore, a 8.1 Manager managing 8.2 Sensors is not a valid scenario. Similarly, the Central Manager must be of the same or higher version than the corresponding Managers.

- The latest 8.2 Manager can manage only the I-series, M-series, NS-series, Virtual IPS Sensors, and NTBA devices on the following software versions — 7.1.x.x, 7.5.x.x, 8.0.x.x, 8.1.x.x, and 8.2.x.x. Similarly, an 8.2 Central Manager can manage only 7.1.x.x, 7.5.x.x, 8.0.x.x, 8.1.x.x, and 8.2.x.x Managers.

To use the information in this section, familiarize yourself with the following terms:

- Homogeneous Manager environment — The major version of the Central Manager and all the Managers are the same.

- Heterogeneous Manager environment — At least one Manager is of an earlier major version than the Central Manager.

- Homogeneous device environment — The major version of the Manager and all the devices are the same.

- Heterogeneous device environment — At least one device is of an earlier major version than the Manager.
Upgrade scenarios for heterogeneous environments

Use these scenarios to understand the possible upgrade paths for a heterogeneous environment. Correlate these scenarios with your deployment to derive an upgrade path.

- Though the scenarios predominantly feature only the M-series and NS-series Sensors, an 8.2 Manager can manage the I-series, Virtual IPS Sensors, NTBA, and XC-Cluster devices as well.
- An 8.2 Manager cannot manage N-series (NAC-only) Sensors and M-series Sensors, which have the NAC feature enabled. Review the Important Notes section in Overview on page 4.
- 8.2 device software is available only for M-series Sensors, NS-series Sensors, Virtual IPS Sensors, NTBA Appliances, and XC Cluster Appliances.

The subsequent sections discuss some sample scenarios. Proceed to the appropriate one for your deployment.

Central Manager upgrade scenarios

The following scenarios involve the Central Manager. If you do not have a Central Manager deployed, you can proceed to Manager upgrade scenarios on page 133.

- Upgrade from a homogeneous 7.1, 7.5, or 8.1 Manager environment to a heterogeneous 8.2 Manager environment:
  - Scenario 1 on page 129
  - Scenario 2 on page 130

- Upgrade from a heterogeneous 7.1, 7.5, or 8.1 Manager environment to a heterogeneous 8.2 Manager environment:
  - Scenario 3 on page 131
  - Scenario 4 on page 132

Review Upgrade path for the Central Manager and Manager on page 139 to know the version of the Central Manager that you need to upgrade to 8.2.

Scenario 1

This scenario is about an upgrade from a homogeneous Manager environment to a heterogeneous 8.2 Manager environment managed by an Manager Disaster Recovery (MDR) pair of Central Managers.
The upgrade path for this scenario is as follows:

1. Make sure the Central Managers, Managers, and Sensors meet the minimum required versions to upgrade to the latest 8.2 version. If not, make sure you upgrade them to the required versions before you begin your 8.2 version.

2. Make sure your current Network Security Platform deployment is functioning as configured and without any issues.

3. Upgrade the Central Manager MDR pair to the latest 8.2 version. See How to upgrade the Central Manager? on page 5.

4. Upgrade the required Manager MDR pairs to the latest 8.2 version. See How to Upgrade the Manager? on page 5.

5. Upgrade the required Sensors to the latest 8.2 version. See How to perform signature set and Sensor software upgrade on page 5.

Scenario 2
This scenario is about an upgrade from a homogeneous Manager environment to a heterogeneous 8.2 Manager environment managed by a standalone Central Manager.
The upgrade path for this scenario is as follows:

1. Make sure the Central Manager, Managers, and Sensors meet the minimum required versions to upgrade to the latest 8.2 version. If not, make sure you upgrade them to the required versions before you begin your 8.2 version.

2. Make sure your current Network Security Platform deployment is functioning as configured and without any issues.

3. Upgrade the standalone Central Manager to the latest 8.2 version. See How to upgrade the Central Manager? on page 5.

4. Upgrade the required Managers to the latest 8.2 version. See How to Upgrade the Manager? on page 5.

5. Upgrade the required Sensors managed by the 8.2 Managers. See How to perform signature set and Sensor software upgrade on page 5.

---

### Scenario 3

This scenario is about an upgrade from a heterogeneous Manager environment to a heterogeneous 8.2 Manager environment managed by an MDR pair of Central Managers.
The upgrade path for this scenario is as follows:

1. Make sure the Central Managers, Managers, and Sensors meet the minimum required versions to upgrade to the latest 8.2 version. If not, make sure you upgrade them to the required versions before you begin your 8.2 version.

2. Make sure your current Network Security Platform deployment is functioning as configured and without any issues.

3. Upgrade the Central Manager MDR pair to the latest 8.2 version. See How to upgrade the Central Manager? on page 5.

4. Upgrade the required Manager MDR pairs to the latest 8.2 version. See How to Upgrade the Manager? on page 5.

5. Upgrade the required Sensors to the latest 8.2 version. See How to perform signature set and Sensor software upgrade on page 5.

**Scenario 4**

This scenario is about an upgrade from a heterogeneous Manager environment to a heterogeneous Manager environment in 8.2, managed by a standalone Central Manager.
The upgrade path for this scenario is as follows:

1. Make sure the Central Manager, Managers, and Sensors meet the minimum required versions to upgrade to the latest 8.2 version. If not, make sure you upgrade them to the required versions before you begin your 8.2 version.

2. Make sure your current Network Security Platform deployment is functioning as configured and without any issues.

3. Upgrade the standalone Central Manager to the latest 8.2 version. See How to upgrade the Central Manager? on page 5.

4. Upgrade the required Managers to the latest 8.2 version. See How to Upgrade the Manager? on page 5.

5. Upgrade the required Sensors to the latest 8.2 version. See How to perform signature set and Sensor software upgrade on page 5.

Manager upgrade scenarios
The following scenarios involve the Manager:

- Upgrade from a homogeneous Sensor environment in 7.1, 7.5, or 8.1 to a heterogeneous Sensor environment in 8.2:
  - Scenario 5 on page 133
  - Scenario 6 on page 134

- Upgrade from a heterogeneous Sensor environment in 7.1, 7.5, or 8.1 to a heterogeneous Sensor environment in 8.2:
  - Scenario 7 on page 135
  - Scenario 8 on page 136

See Minimum required Manager version to know the Manager versions that you need to upgrade to the latest 8.2.

Scenario 5
This scenario is about an upgrade from a homogeneous Sensor environment to a heterogeneous Sensor environment in 8.2, managed by an MDR pair of Managers.
The upgrade path for this scenario is as follows:

1. Make sure that Managers and Sensors meet the minimum required versions to upgrade to the latest 8.2 version. If not, make sure that you upgrade them to the required versions before you begin your 8.2 version.

2. Make sure your current Network Security Platform deployment is functioning as configured and without any issues.

3. Upgrade the Manager MDR pair to the latest 8.2 version. See How to Upgrade the Manager? on page 5.

4. Upgrade the required Sensors to the latest 8.2 version. See How to perform signature set and Sensor software upgrade on page 5.

Scenario 6

This scenario is about an upgrade from a homogeneous Sensor environment to a heterogeneous Sensor environment in 8.2, managed by a standalone Manager.
The upgrade path for this scenario is as follows:

1. Make sure the Manager and Sensors meet the minimum required versions to upgrade to the latest 8.2 version. If not, make sure you upgrade them to the required versions before you begin your 8.2 version.

2. Make sure your current Network Security Platform deployment is functioning as configured and without any issues.

3. Upgrade the standalone Manager to the latest 8.2 version. See How to Upgrade the Manager? on page 5.

4. Upgrade the required Sensors to the relevant 8.2 version. See How to perform signature set and Sensor software upgrade on page 5.

### Scenario 7

This section describes the upgrade for a heterogeneous Sensor environment managed by an MDR pair of Managers.

The upgrade path for this scenario is as follows:

1. Make sure Managers and Sensors meet the minimum required versions to upgrade to the latest 8.2 version. If not, make sure you upgrade them to the required versions before you begin your 8.2 version.

2. Make sure your current Network Security Platform deployment is functioning as configured and without any issues.

3. Upgrade the Manager MDR pair to the latest 8.2 version. See How to Upgrade the Manager? on page 5.

4. Upgrade the required Sensors to the latest 8.2 version. See How to perform signature set and Sensor software upgrade on page 5.
Scenario 8
This section describes the upgrade for a heterogeneous Sensor environment managed by a standalone Manager.

The upgrade path for this scenario is as follows:

1. Make sure the Manager and Sensors meet the minimum required versions to upgrade to the latest 8.2 version. If not, make sure you upgrade them to the required versions before you begin your 8.2 version.

2. Make sure your current Network Security Platform deployment is functioning as configured and without any issues.

3. Upgrade the standalone Manager to the latest 8.2 version. See How to Upgrade the Manager? on page 5.

4. Upgrade the required Sensors to the latest 8.2 version. See How to perform signature set and Sensor software upgrade on page 5.
Enhanced Central Manager/Manager user interface

The following are some of the points you must note regarding enhancements in the Central Manager/Manager user interfaces (UI) over the releases:

- From release 7.5, McAfee began phasing out client-side Java for Central Manager and Manager. The objective is to improve overall performance and user experience. Also, from release 7.5, the Central Manager and Manager user interfaces follow a task-based approach. This design gives you the ability to view and drill down into network issues easily throughout the interface. Therefore, if you are upgrading your Central Manager or Manager from a pre-7.5 release, see the Network Security Platform Addendum I to 7.5 Documentation and familiarize yourself with the UI enhancements from release 7.5.

- Most of the features have been enhanced over the releases. So, the corresponding user interfaces have been changed for those enhancements.

- This guide provides information on those enhancements, which have an upgrade impact. However, see Network Security Platform 8.2 guides and online Help for detailed information on functionality and navigation paths in 8.2.

Feature support in a heterogeneous environment

Note the supported features and important points when you work in a heterogeneous environment in Network Security Platform 8.2.

Take note if you are currently using a pre-7.5 Central Manager or Manager. Over the releases, the names of some of the features and their functionality have changed for a better user-experience. The details of these enhancements and changes are available in the upgrade guides and release notes of 7.0, 7.1, and 7.5 releases.

The following are relevant only if your Network Security Platform upgrade is from 7.x to 8.2:

- From release 8.0, additional Snort rule options are supported. See the Network Security Platform-8.0.5.9-8.0.3.10-M-Series-Release-Notes for the list of newly supported rule options. In a heterogeneous Sensor environment, the Snort custom attacks containing these rule options are supported by the 8.x Sensors but not by the 7.1 and 7.5 Sensors. So, a Snort custom attack that showed no errors when you used the Test Compile feature might still fail to compile on 7.1 and 7.5 Sensors.

- The IP Settings page in release 7.5 is renamed as IP Bindings in 8.x. However, the navigation path to this page is the same.

- See Note regarding File Reputation (Artemis) on page 154.

The following pertain to changes in Network Security Platform 8.2 when compared to the earlier 8.x versions:

- See Inclusion of reconnaissance correlation attack definitions in IPS policies on page 165.

- See Notes regarding Advanced Malware Policies on page 175.

- See Performance and usability enhancements in Manager 8.2 on page 166.

Heterogeneous support for NTBA devices

You can manage a heterogeneous NTBA environment using Manager 8.2.
Notes:
- In this section, the term NTBA device refers to physical as well as virtual NTBA.
- In the context of NTBA, a heterogeneous environment means 7.1, 7.5, 8.0, and 8.1 NTBA devices managed by Manager 8.2.

This note is applicable only if you have NTBA devices on 7.1 and 7.5 managed by a Manager on 8.2. For 7.1 NTBA, the minimum version required for a heterogeneous NTBA environment is 7.1.3.26. For 7.5 NTBA, the minimum version required for a heterogeneous NTBA environment is 7.5.3.35.

Table 11-1  Supported heterogeneous combinations

<table>
<thead>
<tr>
<th>Manager version</th>
<th>Sensor version</th>
<th>Supported NTBA versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2</td>
<td>7.1</td>
<td>• 7.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 7.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 8.0</td>
</tr>
<tr>
<td></td>
<td>7.5</td>
<td>• 7.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 7.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 8.0</td>
</tr>
<tr>
<td></td>
<td>8.0</td>
<td>• 7.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 7.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 8.0</td>
</tr>
<tr>
<td></td>
<td>8.1</td>
<td>• 7.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 7.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 8.0</td>
</tr>
<tr>
<td></td>
<td>8.2</td>
<td>• 7.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 7.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 8.0</td>
</tr>
</tbody>
</table>

Notes:
- If the Sensor version is 7.1 and NTBA version is 7.5 or later, the antimalware and network forensics features are not supported.
- If the Sensor version is earlier than 8.2 and NTBA version is 8.2, the network forensics feature is not supported.

Heterogeneous environment for XC Cluster

You can manage 7.1, 7.5, 8.0, and 8.1 M-8000XC Sensors using the 8.2 Manager. However, if you plan to upgrade the Sensors belonging to a cluster, you must upgrade all of them to 8.2.
How to upgrade the Central Manager?

If you have the Central Manager deployed, you must upgrade it to 8.2 before you upgrade the corresponding Managers. That is, the Central Manager must be of the same or a higher version than the corresponding Managers.

This chapter provides detailed explanation on how to upgrade the Central Manager to the latest 8.2. If you have not deployed a Central Manager, proceed to How to Upgrade the Manager? on page 5.

Contents
- Upgrade requirements for the Central Manager
- Preparation for the upgrade
- Central Manager and operating system upgrade
- MDR Central Manager upgrade
- Standalone Central Manager upgrade

Upgrade requirements for the Central Manager

This chapter discusses the requirements for a successful Central Manager upgrade.

Upgrade path for the Central Manager and Manager

A direct upgrade to Central Manager or Manager 8.2 from versions earlier than what is mentioned in this section is not supported.

⚠️ If you are using a hotfix release, contact McAfee support for the recommended upgrade path.

Table 12-1  Required Central Manager/Manager versions

<table>
<thead>
<tr>
<th>Central Manager / Manager major version</th>
<th>Minimum required version to upgrade to the latest 8.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>7.1.5.15</td>
</tr>
<tr>
<td>7.5</td>
<td>• 7.5.3.11</td>
</tr>
<tr>
<td></td>
<td>• 7.5.5.7</td>
</tr>
<tr>
<td>8.1</td>
<td>• 8.1.7.5</td>
</tr>
<tr>
<td></td>
<td>• 8.1.7.13</td>
</tr>
<tr>
<td>8.2</td>
<td>8.2.7.25</td>
</tr>
</tbody>
</table>
Central Manager and Manager system requirements

Underpowered and/or undersized machines can lead to performance issues and storage problems. We strongly recommend the use of server-class hardware that exceeds the minimum system requirements outlined in this section.

These suggestions do not take into account the amount of disk space you require for alert and packet log storage. See the McAfee Network Security Platform Manager Administration Guide for suggestions on calculating your database capacity requirements.

The following table lists the 8.2 Manager server requirements:

<table>
<thead>
<tr>
<th>Minimum required</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating system</strong></td>
<td>Any of the following:</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 Standard or Enterprise Edition, English operating system, SP1 (64-bit) (Full Installation)</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 Standard or Enterprise Edition, Japanese operating system, SP1 (64-bit) (Full Installation)</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Standard Edition (Server with a GUI) English operating system</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Standard Edition (Server with a GUI) Japanese operating system</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Datacenter Edition (Server with a GUI) English operating system</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Datacenter Edition (Server with a GUI) Japanese operating system</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2 Standard Edition operating system.</td>
</tr>
<tr>
<td><strong>Memory</strong></td>
<td>8 GB</td>
</tr>
<tr>
<td></td>
<td>8 GB or more</td>
</tr>
<tr>
<td><strong>CPU</strong></td>
<td>Server model processor such as Intel Xeon</td>
</tr>
<tr>
<td></td>
<td>Same</td>
</tr>
<tr>
<td><strong>Disk space</strong></td>
<td>100 GB</td>
</tr>
<tr>
<td></td>
<td>300 GB or more</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>100 Mbps card</td>
</tr>
<tr>
<td></td>
<td>1000 Mbps card</td>
</tr>
<tr>
<td><strong>Monitor</strong></td>
<td>32-bit color, 1440 x 900 display setting</td>
</tr>
<tr>
<td></td>
<td>1440 x 900 (or above)</td>
</tr>
</tbody>
</table>

You need Windows Administrator permission for the server machine.

The McAfee Network Security Platform Troubleshooting Guide provides a number of pre-installation tips and suggestions with which McAfee recommends you familiarize yourself before you begin your upgrade. If you run into any issues, we suggest you to check this guide for a possible solution.

The following are the system requirements for hosting Central Manager/Manager server on a VMware platform.
Table 12-2 VMware ESX server requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum</th>
</tr>
</thead>
</table>
| Virtualization software | • ESXi 5.0  
                      | • ESXi 5.1  
                      | • ESXi 5.5                                                                 |
| CPU                  | Intel Xeon® CPU ES 5335 @ 2.00 GHz; Physical Processors – 2; Logical Processors – 8; Processor Speed – 2.00 GHz |
| Memory               | Physical Memory: 16 GB                                                  |
| Internal Disks       | 1 TB                                                                    |

Table 12-3 Virtual machine requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Any of the following:</td>
<td>Windows Server 2012 R2 Standard Edition operating system.</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 Standard or Enterprise Edition, English operating system, SP1 (64-bit) (Full Installation)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 Standard or Enterprise Edition, Japanese operating system, SP1 (64-bit) (Full Installation)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Standard Edition (Server with a GUI) English operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Standard Edition (Server with a GUI) Japanese operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Datacenter Edition (Server with a GUI) English operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Datacenter (Server with a GUI) Japanese operating system</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB</td>
<td>8 GB or more</td>
</tr>
<tr>
<td>Virtual CPUs</td>
<td>2</td>
<td>2 or more</td>
</tr>
<tr>
<td>Disk Space</td>
<td>100 GB</td>
<td>300 GB or more</td>
</tr>
</tbody>
</table>

Preparation for the upgrade

After you make sure you meet the requirements, prepare for the upgrade.

Before you begin the upgrade, make sure that no processes related to McAfee® Network Security Platform (such as automated database archival) are scheduled during the upgrade time frame. Any such concurrent activity might cause conflicts and result in upgrade failure.
Review the upgrade considerations
Review this section carefully before you commence the Central Manager upgrade process.

- **Central Manager upgrade downtime window** — How long the upgrade takes depends on the size of your deployment and the size of your database. The Central Manager upgrade process alone can take an hour to complete.

- **Operating system upgrade downtime** — The latest Central Manager 8.2 is supported on various Windows operating systems as mentioned in Central Manager and Manager system requirements on page 140.
  
  If you want to upgrade the operating system of your Central Manager server, for example from Windows Server 2008 R2, SP1, Standard or Enterprise Edition (Full Installation) to Windows Server 2012 Standard (Server with a GUI), you must factor this in when you estimate the Central Manager downtime.

- **Database backup before and after upgrade** — It is critical that you perform a full backup of your database using the All Tables as well as Config Tables options both before and after the upgrade. Backing up before upgrading enables you to roll back to your earlier version should you encounter problems during upgrade. Backing up immediately following upgrade preserves your upgraded tables and provides a baseline of the 8.2 database that you upgraded to. Importantly, when you are backing up the database, there should not be any scheduled task running in the background.
  
  You cannot restore the database from a lower version Central Manager on a higher version.

- See Change in the default database character set on page 142.

- If it is an upgrade from 7.1, see Note regarding Manager Users and Roles on page 150.

- If it is an upgrade from 7.1 or 7.5, see Change in the default database character set on page 142.

- See Notes regarding scheduled file and database pruning on page 163.

- See Inclusion of reconnaissance correlation attack definitions in IPS policies on page 165.

- See the sections applicable to Central Manager in Performance and usability enhancements in Manager 8.2 on page 166.

- See Enhancements in the Manager Reports on page 164.

### Change in the default database character set

From release 7.5, the default character set of Central Manager and Manager is UTF-8. When you upgrade to 7.5 and later, all Central Manager / Manager tables, including the database, are migrated from Latin-1 character set to UTF-8. Any user-defined table in the Central Manager / Manager database is not affected. Post-upgrade, for the new user-defined tables, the default character set is UTF-8 unless you explicitly define a different character set.

### Backing up Network Security Platform data

Before you upgrade, back up your tables and save any McAfee custom attacks (formerly UDS) that you have created. If you have a very large number of alerts and packet logs to upgrade, first consider archiving and deleting any alert and packet log data that you do not need before creating your database backup files.

Save your entire backup in a different location than the current Central Manager or Manager to prevent data loss.
After you back up the Network Security Platform data, you can consider purging the Manager tables. Details on how to purge the database tables are in the *Network Security Platform Manager Administration Guide*.

Purging the database tables can significantly shorten the Manager upgrade window. If you need the older alerts and packet logs, you can restore the database backup on an offline Manager server for viewing and reporting on that data.

**Perform a database backup**

Back up your database before you upgrade. McAfee strongly recommends the following.

- All tables backup
- Config tables backup
- Archiving alerts and packet logs

All tables backup is time consuming (based upon the size of your database); however, it guarantees the integrity of your existing data. All tables backup includes the entire database, that is, all configurations, user activity, alert information, and custom attacks. However, McAfee recommends a separate all tables and config tables backup. This provides you options if for some reason you want to roll back to your earlier version of the Central Manager or Manager.

**Notes:**

- Preferably, stop the Central Manager or Manager service before you begin any backup process.
- For step-by-step information on all tables and config tables backup as well as archiving alerts and packet logs, see the *McAfee Network Security Platform Manager Administration Guide*.

**Back up McAfee custom attacks**

If you have McAfee custom attacks, back them up prior to upgrade. Refer to the corresponding version of the *McAfee Network Security Platform Custom Attacks Guide* for information on how to back up custom attacks from the Central Manager and Manager.

---

**Central Manager and operating system upgrade**

If you are considering an operating system upgrade as part of the 8.2 Central Manager upgrade, review the methods discussed under *Operating system upgrade scenarios* on page 180.

**MDR Central Manager upgrade**

**Before you begin**

Make sure both the Central Managers meet the required system requirements as mentioned in *Central Manager and Manager system requirements* on page 140.

This section provides the steps to upgrade the primary and secondary Central Managers configured for Manager Disaster Recovery (MDR).


**Task**

1. Using the **Switch Over** feature, make the secondary Central Manager active.
   - If your current Manager version is earlier than 7.5, select *My Company* | *Central Manager* | *MDR* | Manager Pair.
   - For 7.5 and later, click *Manage* and select the root admin domain. Then go to *Setup* | *MDR* | Switch Over.

2. Upgrade the primary Central Manager to the latest 8.2 version.
   For information, see *Standalone Central Manager upgrade* on page 144.

3. If not done already, upgrade to the latest 8.7 signature set in the primary, active Central Manager.
   See *Upgrade the signature set for the Central Manager* on page 146.

4. Bring up the upgraded primary Central Manager.
   The primary is up in standby mode.

5. Stop the secondary Central Manager.
   Because the versions of the primary and secondary Central Manager are now different, you must stop the secondary; else you cannot complete the next step.

6. Using the **Switch Back** feature, make the primary the active Central Manager.

7. Upgrade the secondary Central Manager to the latest 8.2 version.

8. Bring up the upgraded secondary Central Manager.
   The secondary is up in standby mode.

---

**Standalone Central Manager upgrade**

---

**Before you begin**

- Your current Network Security Platform infrastructure meets all the requirements discussed in *Upgrade requirements for the Manager* on page 147.
- If you want to upgrade the RAM on the Central Manager server, make sure you do that before you begin the Central Manager upgrade.
- You have reviewed and understood the implications of the upgrade considerations discussed in *Review the upgrade considerations* on page 142.
- You have backed up your current Central Manager data. See *Backing up Network Security Platform data* on page 142.
- You have the latest 8.2 Central Manager installable file at hand. You can download it from the McAfee Update Server. See *Download the Manager/Central Manager executable* on page 24 for information.
• You have your Central Manager MySQL root password available.

• You have stopped all third-party applications such as Security Information and Event Management (SIEM) agents. It is especially important that you stop any such third-party application that communicates with the MySQL database. The Central Manager cannot upgrade the database if MySQL is actively communicating with another application.

If this is an upgrade of a Central Manager in an MDR pair, switch it to standby mode before you proceed. Make sure you are following the steps in MDR Central Manager upgrade on page 143.

**Task**

1. Stop the McAfee Network Security Central Manager service.
   Right-click on the Central Manager icon at the bottom-right corner of your server and stop the service. Alternatively, go to **Windows Control Panel | Administrative Tools | Services**. Then right-click **McAfee Network Security Central Manager** and select Stop.

2. Stop the **McAfee Network Security Central Manager Watchdog** service using the same method as described in step 1.
   
   ! Make sure the McAfee Network Security Manager Database service remains started.

3. Exit the Central Manager tray from the Windows Task Bar.

4. Close all open applications. (If any application is interacting with Network Security Platform, your installation might be unsuccessful.)

5. Move any saved report files from the server to some other location.
   
   The reports are saved at `<Central Manager install directory>\App\REPORTS`.

6. Run the latest 8.2 Central Manager executable.

7. Install the Central Manager as described in Installing the Central Manager on page 41.

8. At the end of the upgrade process, you might be required to restart the server. If prompted, it is highly recommended that you restart the server.
   
   In the Install Complete page of the Installation Wizard, select one of the following:
   
   • Select **Yes, restart my system** to restart the server immediately.
   
   • Select **No, I will restart my system myself** to complete the upgrade process without restarting the server. You can restart the server at a later point in time. Clicking **Done** in the Manager Installation Wizard will start the Central Manager services.

9. Open the Central Manager in a browser.
   
   You might be requested to download the required version of Java Runtime Environment (JRE) if the same or higher version is not present already.

10. Log on to the Central Manager.
    
    You can verify the version in the **Home** page.

11. Check the **Status** page to ensure that the Central Manager database and the Managers are up.

    To complete the Central Manager upgrade, you must upgrade to the latest 8.7 Signature Set. See Upgrade the signature set for the Central Manager on page 146.
Tasks

• Upgrade the signature set for the Central Manager on page 146

Upgrade the signature set for the Central Manager

Task

1. If you have not already done so, download the most recent 8.7 signature set from the McAfee® Network Security Update Server into the Central Manager.

   In the Central Manager, select Manage | Updating | Download Signature Sets. See the McAfee Network Security Platform Manager Administration Guide or the Online Help for the steps.

2. If you created McAfee custom attacks prior to upgrade, verify that those attacks are present in the Custom Attack Editor.

3. Select Manage | Troubleshooting | System Faults to see if Incompatible custom attack fault is raised.

   This fault could be because of Custom Snort Rules that contain unsupported PCRE constructs. See Note regarding custom attacks on page 175.

Signature Set upgrade is now complete for the Central Manager. For a list of currently supported protocols, see KnowledgeBase article KB61036 at mysupport.mcafee.com.

What is the next step?

• In you have an Central Manager MDR, upgrade the secondary Central Manager.

• If you have upgraded both primary and secondary or if you have only a standalone Central Manager, upgrade the corresponding Managers.
This chapter provides detailed explanation on how to upgrade the Manager to the latest 8.2 version. You must upgrade the Manager before you can upgrade the devices.

### Contents
- Upgrade requirements for the Manager
- Preparation for the upgrade
- Operating system upgrade scenarios
- MDR Manager upgrade
- Standalone Manager upgrade

#### Upgrade requirements for the Manager
Verify the requirements for a Manager upgrade.

#### Upgrade path for the Central Manager and Manager
A direct upgrade to Central Manager or Manager 8.2 from versions earlier than what is mentioned in this section is not supported.

> If you are using a hotfix release, contact McAfee support for the recommended upgrade path.

<table>
<thead>
<tr>
<th>Central Manager / Manager major version</th>
<th>Minimum required version to upgrade to the latest 8.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>7.1.5.15</td>
</tr>
<tr>
<td>7.5</td>
<td>• 7.5.3.11</td>
</tr>
<tr>
<td></td>
<td>• 7.5.5.7</td>
</tr>
<tr>
<td>8.1</td>
<td>• 8.1.7.5</td>
</tr>
<tr>
<td></td>
<td>• 8.1.7.13</td>
</tr>
<tr>
<td>8.2</td>
<td>8.2.7.25</td>
</tr>
</tbody>
</table>
Central Manager and Manager system requirements

Underpowered and/or undersized machines can lead to performance issues and storage problems. We strongly recommend the use of server-class hardware that exceeds the minimum system requirements outlined in this section.

These suggestions do not take into account the amount of disk space you require for alert and packet log storage. See the McAfee Network Security Platform Manager Administration Guide for suggestions on calculating your database capacity requirements.

The following table lists the 8.2 Manager server requirements:

<table>
<thead>
<tr>
<th>Minimum required</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Windows Server 2012 R2 Standard Edition operating system.</td>
</tr>
<tr>
<td>• Windows Server 2008 R2 Standard or Enterprise Edition, English operating system, SP1 (64-bit) (Full Installation)</td>
<td></td>
</tr>
<tr>
<td>• Windows Server 2008 R2 Standard or Enterprise Edition, Japanese operating system, SP1 (64-bit) (Full Installation)</td>
<td></td>
</tr>
<tr>
<td>• Windows Server 2012 R2 Standard Edition (Server with a GUI) English operating system</td>
<td></td>
</tr>
<tr>
<td>• Windows Server 2012 R2 Standard Edition (Server with a GUI) Japanese operating system</td>
<td></td>
</tr>
<tr>
<td>• Windows Server 2012 R2 Datacenter Edition (Server with a GUI) English operating system</td>
<td></td>
</tr>
<tr>
<td>• Windows Server 2012 R2 Datacenter Edition (Server with a GUI) Japanese operating system</td>
<td></td>
</tr>
<tr>
<td>Only X64 architecture is supported.</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB or more</td>
</tr>
<tr>
<td>8 GB</td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td>Same</td>
</tr>
<tr>
<td>Server model processor such as Intel Xeon</td>
<td></td>
</tr>
<tr>
<td>Disk space</td>
<td>300 GB or more</td>
</tr>
<tr>
<td>100 GB</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>1000 Mbps card</td>
</tr>
<tr>
<td>100 Mbps card</td>
<td></td>
</tr>
<tr>
<td>Monitor</td>
<td>1440 x 900 (or above)</td>
</tr>
<tr>
<td>32-bit color, 1440 x 900 display setting</td>
<td></td>
</tr>
</tbody>
</table>

You need Windows Administrator permission for the server machine.

The McAfee Network Security Platform Troubleshooting Guide provides a number of pre-installation tips and suggestions with which McAfee recommends you familiarize yourself before you begin your upgrade. If you run into any issues, we suggest you to check this guide for a possible solution.

The following are the system requirements for hosting Central Manager/Manager server on a VMware platform.
Table 13-2  VMware ESX server requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum</th>
</tr>
</thead>
</table>
| Virtualization software | • ESXi 5.0  
                       | • ESXi 5.1  
                       | • ESXi 5.5                                                                 |
| CPU             | Intel Xeon® CPU ES 5335 @ 2.00 GHz; Physical Processors – 2; Logical Processors – 8; Processor Speed – 2.00 GHz |
| Memory          | Physical Memory: 16 GB                                                   |
| Internal Disks  | 1 TB                                                                     |

Table 13-3  Virtual machine requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum</th>
</tr>
</thead>
</table>
| Operating system| Any of the following:  
                       | • Windows Server 2008 R2 Standard or Enterprise Edition, English operating system, SP1 (64-bit) (Full Installation)  
                       | • Windows Server 2008 R2 Standard or Enterprise Edition, Japanese operating system, SP1 (64-bit) (Full Installation)  
                       | • Windows Server 2012 R2 Standard Edition (Server with a GUI) English operating system  
                       | • Windows Server 2012 R2 Standard Edition (Server with a GUI) Japanese operating system  
                       | • Windows Server 2012 R2 Datacenter Edition (Server with a GUI) English operating system  
                       | • Windows Server 2012 R2 Datacenter (Server with a GUI) Japanese operating system  |
| Memory          | 8 GB    |
| Virtual CPUs    | 2       |
| Disk Space      | 100 GB  |

Preparation for the upgrade

After you make sure you meet the requirements, prepare for the upgrade.

Before you begin the upgrade, make sure that no processes related to McAfee® Network Security Platform (such as automated database archival) are scheduled during the upgrade time frame. Any such concurrent activity might cause conflicts and result in upgrade failure.

Review the upgrade considerations

Review this section carefully before you commence the upgrade process.
Manager upgrade downtime window

The time required to upgrade the Manager depends on the size of your deployment and the size of your database. The Manager upgrade process alone can take an hour to complete.

- Operating system upgrade downtime — The latest Manager 8.2 is supported on various Windows operating systems as mentioned in Central Manager and Manager system requirements on page 140. If you want to upgrade the operating system of your Manager server, for example from Windows Server 2008 R2, SP1, Standard or Enterprise Edition (Full Installation) to Windows Server 2012 Standard (Server with a GUI), you must factor this in when you estimate the Manager downtime.

- How a Sensor functions during the upgrade downtime — While the Manager upgrades, the Sensor (which has not yet been upgraded, and which loses connectivity to the Manager during the Manager upgrade) continues to inspect traffic and accumulate the latest alerts (up to 100,000 alerts) while the Manager is offline during upgrade. Note that the Sensor sends these queued alerts to the Manager when it re-establishes connectivity with the Manager after the upgrade.

Database backup (before and after upgrade)

It is critical that you perform a full backup of your database using the All Tables option both before and after the upgrade. Backing up prior to upgrade enables you to roll back to your current version should you encounter problems during upgrade. Backing up immediately following upgrade preserves your upgraded tables and provides a baseline of the 8.2 database that you upgraded to. Importantly, when you are backing up the database, there should not be any scheduled task running in the background. See Backing up Network Security Platform data on page 142.

You cannot restore the database from a lower version Manager on a higher version Manager.

Notes regarding upgrade from 7.1 to 8.2

If you are upgrading from 7.1 to 8.2, first review the notes in this section. Then, review the notes in the following sections:

1 Notes regarding upgrade from 7.x to 8.2 on page 154.
2 Notes regarding upgrade from 7.x or 8.1 to 8.2 on page 162.

Note regarding Manager Users and Roles

This note is relevant only if your current Manager version is 7.1.

- To match with the extensive enhancements, from release 7.5, the Manager has a new and enhanced list of privileges. There is no mapping between the privileges in the earlier releases and the privileges in 7.5 and later.

- The names of the default roles are unchanged in 7.5 and later. However, these roles now have the new privileges assigned to them. To view a comparison between the list of privileges in 7.1 and 7.5, refer to the Network Security Platform 7.5 Addendum I.

- The users, custom roles, and the roles assigned to users are all preserved during the upgrade. However, the upgrade process removes all the privileges assigned to custom roles. This is because of the new privileges in 7.5 and later. Therefore, you must reassign the privileges to your custom roles post-upgrade. Until then those privileges are denied to the corresponding users. Consider a user Jane to whom you have assigned Custom Role 1 prior to upgrade. Assume that you had also assigned a few privileges to Custom Role 1. Post upgrade, Custom Role 1 has no privileges assigned. Unless you reassign the new privileges to Custom Role 1, Jane is denied access to the Manager.
Note regarding QoS policies

This note is relevant only for upgrades from releases earlier than 7.5 with Traffic Management configured.

In release 7.5 and later, the Traffic Management feature is greatly enhanced and referred to as Quality of Service (QoS). The enhancements are as follows:

- In the earlier releases, you enable the Traffic Management feature at the Sensor level. Then you configure the criteria and the corresponding queues at the port level. From release 7.5.x, QoS is policy-based and similar to the Internal Firewall feature. You define the QoS policy and the component rules for Rate Limiting, DiffServ tagging, and VLAN 802.1p tagging. Then you assign this policy to inline ports. These QoS rules are similar to Firewall rules in functionality.

- QoS Policies are of two types – Advanced and Classic. Advanced QoS policies provide you more options to acutely classify traffic. Classic QoS policies correspond to the Traffic Management feature of the earlier releases.

- In the earlier releases, you specify the Rate limiting queues for each inline port. From release 7.5, the equivalent of Rate Limiting queues are the Rate Limiting Profiles. Functionality wise there is no difference between the Rate Limiting queues of the earlier releases and the Rate Limiting Profiles. You define the Rate Limiting Profiles for an admin domain and apply it to all required inline ports of that domain.

- In the earlier releases, for each inline port, you define queues for DiffServ tagging and VLAN 802.1p tagging. From release 7.5.x, the queues for DiffServ and 802.1p are replaced by firewall-like rules. That is, you define separate sets of rules for DiffServ and 802.1p that the Sensor executes in a top-down fashion. When the traffic matches a rule, the Sensor tags the traffic with the corresponding DiffServ or 802.1p value specified in the rule.

To understand the information in this section, you must be familiar with the Traffic Management feature of earlier releases as well as the QoS feature in 8.x.

Note the change in terminologies from release 7.1:

<table>
<thead>
<tr>
<th>Traffic Management terms in 7.1</th>
<th>Equivalent in 7.5 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Management</td>
<td>Quality of Service (QoS) Policies</td>
</tr>
<tr>
<td>Queue for Rate Limiting</td>
<td>Rate Limiting Profiles and Rate Limiting Rules</td>
</tr>
<tr>
<td>Queue for DiffServ</td>
<td>DiffServ Rules</td>
</tr>
<tr>
<td>Queue for VLAN 802.1p</td>
<td>802.1p Rules</td>
</tr>
</tbody>
</table>

Going forward in this section, the terms Traffic Management and Queues implicitly refer to the feature in Network Security Platform 7.1. The terms QoS, QoS Rules, Rate Limiting Profiles refer to the feature in Network Security Platform 7.5 and later.

Notes:

- When you upgrade the Manager, it identifies the ports where you have configured Traffic Management. For each port that you have configured Traffic Management, it creates an editable Classic QoS Policy that matches with your Traffic Management configuration.

- The Manager creates these policies at the corresponding admin domain and assigns them a random name beginning with TMPolicy.

- The Manager assigns these policies to the corresponding monitoring ports and in the correct direction as well. For example, you had configured Traffic Management for port 7A, which is connected to your inside network. Post-upgrade, the QoS Policy that the Manager created is assigned to 7A-7B/Inbound.
• In a QoS Policy that it created for a port, the Manager includes the rules for each technique. That is, it creates the Rate Limiting Rules for the Rate Limiting Queues. Similarly, it creates the rules for DiffServ and VLAN 802.1p.

• To create these QoS Rules, the Manager uses the default Service Rule Objects for the protocols that you had specified in your Traffic Management configuration. If an equivalent Service Rule Object does not exist, it creates a custom Service Rule Object. For the TCP ports, UDP ports, and IP Protocol Numbers that you had specified, the Manager creates custom Service Rule Objects.

• Consider the Traffic Management Queues as shown in the graphic below. The protocol and port numbers used in the graphic are purely for explanation purpose only.

In the QoS Policy, the Manager creates separate Rate Limiting Rules for each set of Protocols, TCP Port, UDP Port, and IP Protocol Numbers. These rules are created in the same order as indicated in the graphic. Since, the Sensor executes these rules in a top-down fashion, it is important that you understand the order in which these rules are created. You can rearrange this order post-upgrade. Similarly, the Manager creates the rules for DiffServ and VLAN 802.1p tagging.

In a QoS Rule, you can specify only up to 10 Rule Objects for Service. Therefore, only the first 10 Protocols that you specified in the Queue are considered. Similarly, only the first 10 TCP Ports are considered. Therefore, post-upgrade create additional QoS Rules to accommodate the additional Protocols or Port numbers. Also, review these Classic QoS Policies to make sure that your Traffic Management configuration is preserved.

• The Manager creates the QoS policies for every port for which you have configured Traffic Management. Even if the configuration is the same, separate policies are created.

• For all Rate Limiting Queues you defined for a monitoring port, the Manager creates one Rate Limiting Profile. In this Profile, it defines the Classes with the corresponding bandwidth limit. For example, if you had created two Rate Limiting Queues with the values 1024 Kbps and 50 Mbps, the Manager creates a Rate Limiting Profile with Class 1 assigned 1024 Kbps and Class 2 assigned 50 Mbps.

• The Manager names this Profile with a random name starting with QueueProfile. It also assigns this Profile on the corresponding port and in the correct direction.

In Manager 8.2 and later, you can assign QoS policies to Sensor interfaces when you save the QoS policy or through the Policy Manager. This applies to other policies as well.

**Device Profiling**

This note is relevant only for upgrades from releases earlier than 7.5 with OS Fingerprinting configured.
Notes:

- From release 7.5, **OS Fingerprinting** is referred to as **Device Profiling**.
- From 8.0, the options for **Device Profiling** are:
  - **Active Device Profiling** using NTBA.
  - **Passive Device Profiling** using DHCP, TCP, and HTTP profiling techniques.
  - By integrating the Manager with McAfee ePO.
- The navigation path in 8.2 is as follows:
  1. Click the **Devices** tab.
  2. Select the domain from the **Domain** drop-down list.
  3. On the left pane, click the **Devices** tab.
  4. Select the device from the **Device** drop-down list.
  5. Select **Setup** | **Advanced** | **Passive Device Profiling** for Sensors. For NTBA, select **Setup** | **Active Device Profiling**.
- After upgrade of both the Manager and the Sensor, the **OS Fingerprinting** option name changes to **Passive Device Profiling**, with TCP profiling technique selected and enabled device wide. For the other fields such as **Profile Expiration**, the default values apply.
- In the earlier releases, you can only enable **OS Fingerprinting** at the Sensor level. In 7.5 and later, you configure **Device Profiling** at the Sensor level and enable it for the required interfaces and subinterfaces.
- From 8.2, you enable passive device profiling in the **Traffic Inspection** tab of an Inspection Option policy and apply that Inspection Option policy to the required interfaces and subinterfaces.

**Note on Alert Relevance**

This note is relevant only for upgrades with **Relevance** enabled.

Notes:

- The **Relevance** feature is referred to as **Alert Relevance** in release 7.5 and later.
- The navigation path in the 8.x Manager is as follows:
  1. Click **Manage** and select the **Domain**.
  2. Select **Integration** | **Vulnerability Assessment** | **Enhancing Alert Relevance** | **Enable**.
- If you had enabled **Relevance Analysis** in the earlier release, post-upgrade **Active Relevance** is enabled.
- Previously, in the Threat Analyzer and Reports, relevance is indicated as relevant, not relevant, or unknown. From release 7.5, relevance is score based.
  Beginning with version 8.0, the Manager displays a default relevance score of 50% in certain conditions. When an attack cannot be assigned a relevance score using conventional methods, the Manager uses the attack signature to identify the application in which the vulnerability exists and which operating systems that application runs on.
  The Manager then correlates the operating system of the affected endpoint with the operating system that the application is compatible with to determine the score. If the two match, a default score of 50% is assigned. If the two do not match, a score of 0% is assigned. For more information, see *Network Security Platform 8.1 IPS Administration Guide*. 
Notes regarding upgrade from 7.x to 8.2

If you are upgrading from 7.1 or 7.5 to 8.2, review the notes in this section. Then, review the notes in Notes regarding upgrade from 7.x or 8.1 to 8.2 on page 162.

Change in the default database character set

From release 7.5, the default character set of Central Manager and Manager is UTF-8. When you upgrade to 7.5 and later, all Central Manager / Manager tables, including the database, are migrated from Latin-1 character set to UTF-8. Any user-defined table in the Central Manager / Manager database is not affected. Post-upgrade, for the new user-defined tables, the default character set is UTF-8 unless you explicitly define a different character set.

Note on Apache Solr

From release 8.0, the Manager uses Apache Solr for quick retrieval of data. Solr is an open-source search platform from the Apache Lucene project. The Manager uses Solr to retrieve data to be displayed in the Manager Dashboard and Analysis tabs. When you upgrade the Manager from 7.x to 8.x, the Manager installation wizard prompts you to specify the location on the Manager server where you want to install Solr. The Solr installation requires at least 20 GB.

If you have 1 million alerts or more, in addition to the two SQL scripts, you must also run a separate script for Solr after you have run Alertproc_offline_2.sql. To run the Solr script, you must stop the Manager service. This script, under test conditions, might take around 2 minutes for 1 million alerts. See Run additional scripts on page 185.

Note regarding File Reputation (Artemis)

From release 8.0, the Custom Fingerprints feature is renamed as Blacklist and Whitelist. If you change the whitelist or blacklist entries, the Manager updates the 8.x Sensors within 5 minutes; for 7.x Sensors in a heterogeneous environment, you must do a configuration update.

In the 8.2 Manager, the Whitelisted and Blacklisted Hashes page is renamed to File Hash Exceptions. In the latest 8.2 Manager, File Hash Exceptions is available at Policy | <domain name> | Intrusion Prevention | Advanced Malware | File Hash Exceptions.

The rest of this note is relevant only for upgrades from release 7.1 with File Reputation configured.

The File Reputation feature in Network Security Platform 7.1 is part of the Advanced Malware policies from release 7.5. So, after you upgrade the Sensors from 7.1 to 8.x, Advanced Malware policies are automatically created with these settings and also applied to the corresponding Sensor interfaces and subinterfaces.

After you upgrade, some of the File Reputation configurations are preserved, but not all. Post-upgrade, review the Advanced Malware policies and change them according to your requirements.

Notes:

- After you upgrade the Manager to 8.x, the Custom Fingerprints, DNS server settings, and HTTP Response Scanning settings are preserved.

- When you upgrade the Sensor to 8.x, the following Advanced Malware policies are created and applied to the corresponding Sensor resources:
  - If you had enabled only GTI File Reputation, an Advanced Malware policy called GTI File Reputation Policy is created.
  - If you had enabled only Custom Fingerprints, an Advanced Malware Policy called Custom Finger Prints Policy is created.
  - If you had enabled both, an Advanced Malware policy called GTI File Reputation and Custom Finger Prints Policy is created.
Regardless of the domain where you have enabled GTI File Reputation or Custom Fingerprints, these policies are created at the root admin domain.

You can customize these policies from the root admin domain.

These policies are created only once. Consider that you enabled GTI File Reputation on resources of two different Sensors. When you upgrade the first Sensor, the GTI File Reputation Policy is created. When you upgrade the second Sensor, the same policy, in its current state, is applied on the resources of the second Sensor as well.

The Sensitivity configuration is not preserved and this field is not available post-upgrade. The Action Thresholds are disabled after the upgrade. For example, if you had enabled blocking prior to upgrade, it is disabled post-upgrade. So, review the Advanced Malware policies after upgrade and make changes as required. In 7.5 and later, you must specify the threshold for each Sensor response action.

In 7.1, you could send a TCP reset to the source of the traffic, destination, or both. In 7.5 and later, if you configure TCP reset, the Sensor sends it to both the source and destination and it is not user-configurable.

In 7.1, you could configure the Sensor response actions separately for GTI File Reputation and Custom Fingerprints. In 7.5 and later, you configure the Sensor response actions (Action Thresholds) based on file type. However, these response actions apply to both GTI File Reputation and Blacklist and Whitelist.

In 7.1, the list of File Types for Custom Fingerprints consisted of file extensions such as exe, doc and pptx. In 7.5 and later, these File Types are categorized as executables, Microsoft Office files, and so on. You only select these categories and not individual file types. In the 3 default upgrade Advanced Malware policies, these categories are automatically selected based on the file types that you had selected in 7.1. For example, if you had selected doc in 7.1, after upgrade the Microsoft Office Files File Type is selected for Blacklist and Whitelist. In 7.1, you could not select the File Types for GTI File Reputation. In 7.5 and later, you can select the required category for File Type.

The following table compares the changes to the File Reputation feature in versions 7.1 and 8.x:

<table>
<thead>
<tr>
<th>Feature name</th>
<th>Network Security Platform 7.1</th>
<th>Network Security Platform 8.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Reputation - Custom Fingerprints</td>
<td>Blacklist and Whitelist in Advanced Malware policies.</td>
<td>TIE / GTI File Reputation in Advanced Malware policies.</td>
</tr>
<tr>
<td>File Reputation - GTI Fingerprints</td>
<td>• You configure this at Admin Domain</td>
<td>• For a Domain, click Devices and select the Domain. Then go to Global</td>
</tr>
<tr>
<td></td>
<td>Device List</td>
<td>Common Device Settings</td>
</tr>
<tr>
<td></td>
<td>Misc</td>
<td>Name Resolution.</td>
</tr>
<tr>
<td>DNS server settings</td>
<td>• This DNS server configuration applies to GTI File Reputation (Artemis), Firewall, and NTBA.</td>
<td>• For a Sensor, click Devices and select the Domain. Then click Devices and select the Device. Then go to Setup</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Name Resolution.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• This DNS server configuration applies all features that require the Manager or the Sensor to communicate with the DNS server.</td>
</tr>
<tr>
<td>Response Action</td>
<td>Network Security Platform 7.1</td>
<td>Network Security Platform 8.2</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>• You configure the response in the File Reputation Attacks using the Policy Editor.</td>
<td>You configure the Sensor response actions, such as blocking and TCP reset, in the Advanced Malware policies (in the Action Thresholds section). These options are not available in the IPS malware attack definitions.</td>
<td></td>
</tr>
<tr>
<td>• For File Reputation, configure the response in the Malware: Potential Malicious File Transfer Detected by GTI File Reputation (Artemis) attack.</td>
<td>For the Manager response actions, such as Email notification, you use the same attack definitions as in 7.1.</td>
<td></td>
</tr>
<tr>
<td>• For Custom Fingerprints, configure the response in Malware: Potential Malicious File Transfer Detected by Custom Fingerprint attack.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enabling the feature

You can even enable GTI File Reputation and Custom Fingerprints at the interface and subinterface levels.

You can assign the different Advanced Malware policies for the interfaces and subinterfaces.

**Manager 8.2 managing a Sensor on 7.1**

In release 7.1, there are two options related to malware detection: **File Reputation - Custom Fingerprints** and **File Reputation - GTI Fingerprints**. Both these options are available as part of **Protection Options**. From release 7.5, these **File Reputation** options are part of Advanced Malware Policies.

Consider that you have a Manager 7.1 managing a Sensor running on 7.1 and you have configured the File Reputation options. When you upgrade the Manager to 8.2, an inspection option policy is created with the File Reputation options preserved. These File Reputation options are available in the **Legacy Malware Detection** tab of the inspection option policy.

Assume that different File Reputation configurations are applied to interfaces 1A-1B and 2A-2B. Therefore, during the Manager upgrade, the Manager creates two inspection option policies and applies these policies to the corresponding interfaces. Until you upgrade this 7.1 Sensor, you use the **Legacy Malware Detection** tab in these inspection option policies to manage the File Reputation settings. The path to inspection option policies is `Policy | <domain name> | Intrusion Prevention | Inspection Options Policies`.

Later, when you upgrade the 7.1 Sensor to 8.2, the Manager creates Advanced Malware policies based on the settings in the **Legacy Malware Detection** tab. The Manager also applies these Advanced Malware policies to the corresponding Sensor resources. So, post upgrade, you use the Advanced Malware policies to manage these settings. Regardless of the domain where you enabled the File Reputation options in Manager 7.1, the default Advanced Malware policies are created at the root admin domain.

Post upgrade to 8.2, review the Advanced Malware policies to make sure that your pre-8.2 configuration is preserved.

**Performance and usability enhancements from Manager 8.0**

McAfee is in the process of migrating away from client-side Java for the Manager. The objective is to improve the Manager’s performance and user experience. As a result, the navigation path, feature name, and option names are changed in some cases.

**Top Applications**

From 8.0, the **Top Applications** monitor has been moved from the **Threat Analyzer** to the **Dashboards** page. The monitor can provide application summary for a specified time. In the **Top Applications** monitor, you can:

- Toggle between attacks, bytes, and connections.
- Toggle between any risk and high risk (an icon is displayed to indicate if it is a high risk).
NTBA Traffic Monitors

Three existing traffic-related NTBA monitors are moved out of the Threat Analyzer:

- Bandwidth Utilization (%) - Interface
- Throughput Enterprise Traffic (Bytes)
- Traffic Volume (Bytes) - Zone

These monitors are now available in Devices | <admin domain name> | Devices | <NTBA Appliance> | Troubleshooting | Traffic Throughput.

These monitors provide data per NTBA appliance, which can be used to check if traffic is going through the device (default), a zone, or an exporter interface.

For more information, refer to the Manager Administration Guide and NTBA Administration Guide.

Non-standard port validation through signature set

This note is applicable only for upgrades from 7.x.

From release 8.0, Network Security Platform validates standard ports used across various protocols using the signature set. If the assigned non-standard port is a standard port for another protocol, the Manager displays an error message prompting you to enter a different port number. If you upgrade to 8.x from an older version of the Manager, and if there is a conflict between the non-standard port assigned and the standard port in the signature set, the signature set update will fail. In this scenario, manually update the conflicting port number. For more information, refer to the Manager Administration Guide.

Note regarding assigning policies at the admin-domain level

In the earlier releases, to assign IPS and reconnaissance policies at an admin-domain level, you could use the Policy Assignments page (Devices | <Domain Name> | Global | Default Device Settings | IPS Devices | Policy Assignments).

In Manager 8.2 and later, you can assign the policies directly to Sensor interfaces. Use the Policy Manager or click in the Assignments column in the corresponding policies page. For more information assigning policies, refer to the Network Security Platform IPS Administration Guide. Also, see the note on reconnaissance policies - Inclusion of reconnaissance correlation attack definitions in IPS policies on page 165.

Performance and usability enhancements from Manager 8.1

McAfee is in the process of migrating away from client-side Java for the Manager. The objective is to improve the Manager’s performance and user experience. As a result, the navigation path, feature name, and option names are changed in some cases.

The following features are enhanced from Manager 8.1:

- Policy | <Domain name> | Intrusion Prevention | Firewall Policies
- Policy | <Domain name> | Intrusion Prevention | QoS Policies
- Policy | <Domain name> | Intrusion Prevention | Connection Limiting Policies
- Policy | <Domain name> | Intrusion Prevention | Objects | Quarantine Zones (was earlier Policy | Intrusion Prevention | IPS Quarantine | Network Access Zones)
- Devices | <Domain name> | Devices | <Device Name> | Troubleshooting | Denial of Service | Profiles
**Note on IPS Quarantine**

To further improve user-experience, menu and terminology changes have been made to the IPS Quarantine feature from release 8.1. There is no change in the Sensor’s ability to quarantine attacking hosts. This section details the changes regarding IPS Quarantine with respect to usability, menu navigation, and terminology changes.

- From release 8.0, no McAfee NAC notification or host-type-based quarantine is available.
- Since Network Access Control (NAC) is not available from release 8.1, common configurations such as NAZ and NAC Exclusion List now apply only to IPS Quarantine.

<table>
<thead>
<tr>
<th>Table 13-4 Terminology changes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Terms prior to 8.1</strong></td>
</tr>
<tr>
<td>IPS Quarantine</td>
</tr>
<tr>
<td>Network Access Zones (NAZ)</td>
</tr>
<tr>
<td>NAC Exclusion List</td>
</tr>
<tr>
<td>Host</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 13-5 Navigation changes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
</tr>
<tr>
<td>Manage rule objects.</td>
</tr>
<tr>
<td>Forward quarantine rule matches to a syslog server (admin-domain configuration).</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Forward quarantine rule matches to a syslog server (Sensor-level configuration).</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Action</td>
</tr>
<tr>
<td>--------</td>
</tr>
</tbody>
</table>
| Customize quarantine browser message | Page name: Browser messages  
Path: Policy | <domain_name> | Intrusion Prevention | IPS Quarantine | Browser messages | Page name: Browser messages  
Path: Devices | <domain_name> | Global | IPS Device Settings | Quarantine | Browser Messages |
| Configure Remediation Portal settings | Page name: Remediation Portal  
Path: Policy | <domain_name> | Intrusion Prevention | IPS Quarantine | Remediation Portal | Page name: Remediation Portal  
Path: Devices | <domain_name> | Global | IPS Device Settings | Quarantine | Remediation Portal |
| View the quarantine summary for an admin domain | Page name: Summary  
Path: Policy | <domain_name> | Intrusion Prevention | IPS Quarantine | Summary | Page name: Summary  
The Summary page for the admin domain is deprecated in the 8.2 Manager. |
| Manage quarantine settings for an admin domain using the Quarantine Wizard | Page name: IPS Quarantine Configuration Wizard  
Path: Policy | <domain_name> | Intrusion Prevention | IPS Quarantine | Default Port Settings | Page name: Quarantine Configuration Wizard  
Path: |
1. Click the Devices tab. 
2. From the Domain drop-down list, select the domain you want to work in. 
3. Click the Global tab. 
4. Select IPS Device Settings | Quarantine | Default Port Settings. |
Table 13-5 Navigation changes (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Prior to 8.1</th>
<th>In 8.1 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the quarantine summary for a Sensor</td>
<td>Page name: Summary Path: 1 Click the Devices tab. 2 From the Domain drop-down list, select the domain you want to work in. 3 On the left pane, click the Devices tab. 4 Select the device from the Device drop-down list. 5 Select Policy</td>
<td>Page name: Summary Path: 1 Click the Devices tab. 2 From the Domain drop-down list, select the domain you want to work in. 3 On the left pane, click the Devices tab. 4 Select the device from the Device drop-down list. 5 Select Setup</td>
</tr>
</tbody>
</table>

| Enable quarantine for an inline monitoring port | Page name: Port Settings Path: 1 Click the Devices tab. 2 From the Domain drop-down list, select the domain you want to work in. 3 On the left pane, click the Devices tab. 4 Select the device from the Device drop-down list. 5 Select Policy | Page name: Port Settings Path: 1 Click the Devices tab. 2 From the Domain drop-down list, select the domain you want to work in. 3 On the left pane, click the Devices tab. 4 Select the device from the Device drop-down list. 5 Select Setup | |

Note on McAfee NAC Notification

The McAfee NAC Notification checkbox is removed from the following windows:
- Edit exploit attack detail: Policy | Intrusion Prevention | IPS Policies
- Edit Reconnaissance attack detail: Policy | Intrusion Prevention | Advanced | Default IPS Attack Settings
- Bulk Edit exploit attack detail: Policy | Intrusion Prevention | IPS Policies
- Bulk Edit Reconnaissance attack detail: Policy | Intrusion Prevention | Advanced | Default IPS Attack Settings

Therefore, if you had enabled this option in the earlier version, these are permanently removed post-upgrade. For more information, see the Manager Administration Guide.

Scheduling signature set and botnet detectors download separately

Prior to 8.1, scheduling for downloading or deploying of both signature sets and botnet detectors has to be done together under Manage | Updating | Automatic Downloading and Deployment page.

From 8.1, the Manager provides the flexibility to separately schedule download and deploying of IPS signature sets and botnet detectors.
From 8.2, **IPS Signature Sets** is renamed as **Signature Sets** and **Botnet Detectors** is renamed as **Callback Detectors**. Because of these terminology changes, other relevant options and page names in the Manager are also renamed accordingly.

- **Signature sets**: Manage | <root admin domain> | Updating | Automatic Updating | Signature sets
- **Callback detectors**: Manage | <root admin domain> | Updating | Automatic Updating | Callback Detectors

From release 8.1, the automatic signature set deployment applies to the corresponding Sensors and NTBA Appliances.

**NTBA-related enhancements from release 8.1**

**Whitelisted and Blacklisted Hashes enhancements**

Earlier, the auto-blacklisted executable hashes were added to the Manager global list. In addition, auto-whitelisted executable hashes are also sent to the Manager global list. You can view these in the Policy | <root admin domain name> | Intrusion Prevention | Advanced Malware | File Hash Exceptions page.

> If the executables are auto-whitelisted in 8.0, after upgrading to 8.2, NTBA will reclassify these executables. The new classification values are sent to the Manager.

**Physical Ports page enhancements**

The Devices | <domain name> | Devices | <NTBA Appliance> | Setup | Physical Ports | Monitoring Ports is renamed to Collection Ports. Likewise, monitoring ports will now be called collection ports for NTBA.

The IP settings were previously configured on the Collection Port Settings page, which is now removed. These can be now set on the Devices | <domain name> | Devices | <NTBA Appliance> | Setup | Physical Ports page.

Additional columns for speed and IP address for a collection port are displayed in Physical Ports/Collection Ports. Port status displays whether a port is Up, Down, or Disabled. You can set the speed and IP address for each collection port. For virtual NTBA appliances, the assigned network adapters are displayed.

**Management port enhancements**

From release 8.1, you can configure the NTBA management port to receive NetFlows. If none of the collection ports are configured in the earlier version, post-upgrade the management port is selected by default. This enables you to use an IP address or port that is already up and running.

**NTBA Integration page enhancements**

The option to set the IPS Sensor as an exporter for NTBA was available on the Exporting page. This page is removed in the Manager from release 8.1.

You can now directly configure these settings from the Devices | <Domain name> | Devices | <IPS Sensor> | Setup | NTBA Integration page. The NTBA Integration drop-down has options to enable integration for flow exporting and advanced malware analysis. You can use the View Connectivity button to view data about records sent between the IPS Sensor and the configured NTBA Appliance. You can view ports that are up and assigned IP addresses to easily configure ports for integration.

When NTBA integration is enabled for an IPS Sensor and set to **Enabled for Advanced Malware Analysis Only**, you only need to select a target NTBA Appliance.

> If NTBA was integrated with a Sensor, and you upgrade from 7.5 or 8.1 to 8.2, the NTBA Integration option must show **Enabled for Flow Exporting and Advanced Malware Analysis** as selected. If you upgrade from 7.1 to 8.2, it must display **Enabled for Flow Exporting only**.
Zone definition enhancements

Earlier, to add a new zone element, you defined an element in the Add Zone Element window. This page is removed from the 8.1 release.

You can now define the inside and outside zones, and zone elements by selecting Devices | <admin domain> | Devices | <NTBA Appliance> | Zones.

This page has a lower panel that allows you to add multiple elements for an interface type for a zone.

Static route enhancements

In 8.0, you could define a static route from the Devices | <admin domain name> | Devices | <NTBA Appliance> | Setup | Advanced | Static Routes page. From 8.1, this page is placed directly under Setup and renamed as Routing page.

You can view the collection port status and assigned IP address while you define a route. You can configure static routes on an NTBA Appliance for diagnostic purposes and to check for connectivity between NTBA and IPS Sensor ports. A static route is also required if you want to route outbound traffic from a collection port.

Communication rule enhancements

Earlier, the Policy | Network Threat Behavior Analysis | NTBA | New/View/Edit | Communication Rules | New | Traffic to Match | View/Edit, the Edit Matched Traffic page had qualifiers that you could select to trigger alerts when traffic matched those conditions. The Equal To and Not Equal To qualifiers are removed to simplify and assume that traffic must always be equal to the selected value.

If you upgrade from 7.1 or 7.5 to 8.2, the communication rules that have Not Equal To qualifiers are removed. Only the rules that have Equal To qualifier for the matched condition are retained.

Update server location

The update server location is changed from wpm.webwasher.com to tau.mcafee.com to download the anti-malware updates.

Notes regarding upgrade from 7.x or 8.1 to 8.2

Review the following subsections if you are upgrading the Manager from 7.1, 7.5, or 8.1 to 8.2.

Note on McAfee GTI participation

This note is relevant only for upgrades with McAfee GTI participation configured.

McAfee TrustedSource feature is referred to as McAfee IP Reputation from release 7.5. Your McAfee GTI participation configuration is maintained post-upgrade. However, after you upgrade, some additional information is shared with McAfee. So, after the upgrade select Manage | Integration | Global Threat Intelligence. Then click on the Show Me What I'm Sending link and review the information that you are sharing with McAfee. If required, modify the McAfee GTI participation accordingly. In an MDR pair, the Show Me What I'm Sending link is available only in the active Manager.

There is a row at the bottom of the page to check whether your Manager is communicating with the McAfee GTI server.
Notes regarding scheduled file and database pruning

• In Manager 8.2, Automated Pruning is renamed as File and Database Pruning.

• When you upgrade, the scheduler configuration from the Automated Pruning page is preserved. However, your pruning configuration (Enabled? and Prune...) are lost. Instead, pruning is enabled for all the File Types with the default prune age. So, after upgrade, make sure the File and Database Pruning configuration is as per your requirement.

• In release 8.2, the menu structure and many option names under Maintenance (Manage | <root admin domain> | Maintenance) are modified compared to earlier releases. For the details of these changes, refer to Network Security Platform 8.2 Release Notes.

• Prior to release 8.2, application visualization data is stored both in Apache Solr and MySQL. In the earlier releases, Apache Solr stored only the last 14 days’ application visualization data. As for the application visualization data stored in MySQL, you could configure automatic pruning in the Automated Pruning page.

From release 8.2, application visualization data is stored only in Apache Solr. Therefore, the File and Database Pruning page in the 8.2 Manager, does not have options to enable pruning of application visualization data.

In release 8.2, you can specify the pruning settings for alerts and application visualization data stored in Apache Solr.

1 Select Manage | <root admin domain> | Maintenance | Database Pruning | Alert Pruning to navigate to the Alert Pruning page.

2 Specify the maximum number of application visualization data records you want to store in the Maximum Alerts to Store for Dashboard Data. Note that the Maximum Alerts to Store for Dashboard Data option separately applies to both alerts and application visualization records stored in Apache Solr. For example, if you specify 10,000 as the value, then the Manager saves only the latest 10,000 alerts and the latest 10,000 application visualization records in Apache Solr. Note that Maximum Alerts to Store for Dashboard Data option applies only to data stored in Apache Solr. Also, the Manager Dashboard fetches information only from Apache Solr and not MySQL.

• In the 8.2 Manager, the Alert Data Pruning page is renamed as Alert Pruning. Your current configuration in the Alert Data Pruning page is preserved during the upgrade.

  • Maximum Alert Quantity option is renamed as Maximum Alerts to Store for Report Data.

  • Maximum Alert Age option is renamed as Maximum Alert Age for Report Data.

• To access the Malware Archive page in the 8.2 Manager, select Manage | <root admin domain> | Maintenance | Malware Archive.

Enhancements in the Central Manager and Manager Dashboard

The following are the changes in the Manager Dashboard from release 8.2:

Update Status monitor:

• Update Status monitor is enhanced and renamed as Device Summary monitor.

• The Device Summary monitor displays information related to devices. The Manager Summary monitor displays information related to the Manager. Therefore, information such as the active signature set and callback detector versions on the Manager are now displayed in the Manager Summary monitor.

• The Update Status link, which was available in the older Update Status monitor is not available in the new Device Summary monitor. However, if changes are pending for a device, click on the Changes pending link to display the Deploy Pending Changes field.
• Note the color-coded icons in the **Device Summary** and **Manager Summary** monitors:
  • Green — Up-to-date; no action required.
  • Red — A newer version is available.
  • Blue — You must deploy the pending changes.

For more information on **Device Summary** and **Manager Summary** monitors, see the *Network Security Platform 8.2 Manager Administration Guide*.

The following are the changes in the Central Manager Dashboard from release 8.2.7.4x:

• Since the connected Managers are treated as devices in the Central Manager, the **Device Summary** monitor displays the synchronization status of connected Managers.

• Similar to the Manager Dashboard, the Central Manager Dashboard also displays color-coded icons to indicate status.

• The signature set version is displayed in the **Manager Summary** monitor.

**Note on Incident Generator**

With release 8.2, the **Incident Generator** in the **Threat Analyzer** is no longer supported by Network Security Platform.

**Enhancements in the Manager Reports**

• **Output format** — In Central Manager and Manager 8.2, you can generate reports in PDF portrait or PDF landscape. If the output format is PDF, the reports generated prior to the upgrade display in the PDF portrait format. Similarly, PDF portrait is set as the report format for automated reports, if the output format is PDF prior to the upgrade.

• Because **Rule Sets** is renamed to **Attack Set Profiles** in release 8.2, the **Rule Set** report is also renamed as **Attack Set Profile** report in Central Manager and Manager.

• In release 8.2, the **Exception Objects** report is relevant only in a heterogeneous Sensor environment. That is, the **Exception Objects** report fetches information only regarding exception reports applied on Sensors on pre-8.2 software. There is no equivalent configuration report for ignore rules. However, you can make use of the **Save as CSV** option in the **Ignore Rules** page. For information on **Exception Objects** and **Ignore Rules**, see Performance and usability enhancements in Manager 8.2 on page 166.

• **Intrusion Policy Configuration** report is deprecated from Central Manager and Manager 8.2. So, if you had scheduled this report, it is not generated post-upgrade.

• The **File Reputation** report is deprecated from Manager 8.2. So, if you had scheduled this report, it is not generated post-upgrade.

**Menu and navigation path changes in Manager 8.2**

As part of Manager enhancements, menu names and navigation paths have changed for multiple features. Some of the critical changes are:

• The sub-menus **Common** and **IPS Devices** under **Default Device Settings** are now available as **Common Device Settings** and **IPS Device Settings**.

• **Alert Acknowledgment** is renamed to **Auto-Acknowledgment** with no change in functionality. To access the **Auto-Acknowledgment** page, select **Policy** | `<domain name>` | **Intrusion Prevention** | **Exceptions** | **Auto-Acknowledgement**.

• In the 8.2 Manager resource tree, **TCP Settings** is renamed as **Protocol Settings** but the navigation path remains the same. Also, in the **Protocol Settings** page, the TCP and UDP parameters are now segregated.
The following options in the Alert Suppression section of the IPS Alerting page are renamed. However, the earlier configuration is preserved during upgrade:

- Maintain __ unique source-destination IP pairs is renamed to Generate unique suppression summary alerts for up to __ attack, attacker and target combinations.

- Send first __ as individual alerts is renamed to Generate standard alerts for the first __ attack(s) seen during the alert suppression window.

- Suppress for __ seconds is renamed to The alert suppression window is __ seconds.


Inclusion of reconnaissance correlation attack definitions in IPS policies

As part of simplifying policy management in release 8.2, reconnaissance policies are deprecated in the Central Manager and the Manager. The IPS policies now include all reconnaissance attack definitions. So, now you can use a single policy to manage exploit and reconnaissance attacks. The added advantage is you can now apply customized reconnaissance correlation attacks per interface.

After you upgrade the Central Manager or Manager to 8.2, merge the attack definitions in your reconnaissance policies to your IPS policies. Information on how to merge reconnaissance policies and IPS policies is provided at the end of this section.

- In case of Central Manager, you can merge the IPS and reconnaissance policies immediately after you upgrade the Central Manager. When the policies synchronize between the Central Manager and the Managers, the reconnaissance attacks in the IPS policies apply only to 8.2 Managers and ignored in the cases of pre-8.2 Managers.

- In the case of Managers, recommend that you merge the IPS and reconnaissance policies when you are ready to upgrade Sensors to 8.2 (that is, after you upgrade the Manager to 8.2). You can merge the policies even after you upgrade the Sensors to 8.2. However, until you merge the reconnaissance and IPS policies, any customizations to reconnaissance attacks done prior to the 8.2 upgrade are ignored. Consider that you enabled e-mail notification for a specific reconnaissance attack prior to upgrade. This customization is ignored until you merge the reconnaissance and IPS policies. The alternative is to re-customize the reconnaissance attack definitions in the IPS policy editor of the 8.2 Manager.

Consider the following Manager scenarios:

- **Scenario 1:** You have 2 customized reconnaissance policies (R1 and R2) and 3 customized IPS policies (IPS-1, IPS-2, and IPS-3). R1 and IPS-1 apply to 1A-1B of Sensor 1; R1 and IPS-2 apply to 2A-2B of Sensor 1; R2 and IPS-3 apply to all interfaces of Sensor 2.
  
  For this scenario, it is recommended that you complete the following before you upgrade a Sensor to 8.2:
  
  1. Consider Sensor 1. R1 is the reconnaissance policy and IPS-1 and IPS-2 are the IPS policies pertaining to this Sensor. So, merge R1 with IPS-1 and IPS-2 and then upgrade the Sensor.
  
  2. Similarly, merge R2 and IPS-3 before you upgrade Sensor 2.

- **Scenario 2:** You have applied R1 and IPS-1 to interfaces of Sensor 1 and R2 and IPS-1 to interfaces of Sensor 2.

  At a time, you can merge only one reconnaissance policy with an IPS policy. In this scenario, you must choose between R1 and R2. The attack definitions from the reconnaissance policy that you last merge are included in the IPS policy.
If you have pre-8.2 Sensors, you must use the **Reconnaissance Policies** page to manage reconnaissance policies and attack customizations. To apply reconnaissance policies to pre-8.2 Sensors, use the **Devices** tab of the **Policy Manager**. The **Reconnaissance** section in the **Devices** tab is available only for pre-8.2 Sensors. So, reconnaissance attacks in the IPS policies apply only to 8.2 Sensors; reconnaissance attacks in the reconnaissance policies apply only to pre-8.2 Sensors.

When there are no more pre 8.2 Sensors in your setup, the **Reconnaissance Policies** option is removed from the Resource Tree. Later, if you add a pre-8.2 Sensor to the Manager, the **Reconnaissance Policies** option is available again.

Complete the following to merge a reconnaissance policy with an IPS policy in the Manager. Follow a similar process for Central Manager:

1. In the Manager or Central Manager, select **Policy** | `<Domain name>` | Intrusion Prevention | Reconnaissance Policies | Reconnaissance Attack Settings Merge Utility. If Reconnaissance Policies option is not available, you can select **Policy** | `<Domain name>` | Intrusion Prevention | Advanced | Reconnaissance Attack Settings Merge Utility.

2. In the **Reconnaissance Attack Settings Merge Utility** page, select the reconnaissance policy to be merged from **Source Reconnaissance Policy** drop-down.

3. Select the IPS policy from the **Target IPS Policy** drop-down.

4. Click **Merge**.

**Performance and usability enhancements in Manager 8.2**

McAfee is in the process of migrating away from client-side Java for the Manager. The objective is to improve the Manager’s performance and user experience. As a result, the navigation path, name, and option names are changed for some of the features.

**Port Settings**

In release 8.0, the **Port Settings** page is enhanced for all devices except I-series Sensors. This page is used to configure the physical port parameters for various network devices added to the Manager. The enhanced **Port Settings** page provides separate tabs for configuring monitoring, response, and management ports. From release 8.1, **Port Settings** in the menu is renamed as **Physical Ports**. This enhanced **Physical Ports** page is available for all devices in the 8.2 Manager except I-series Sensors.

The navigation path to the **Physical Ports** page is **Devices** | `<Admin Domain>` | **Devices** | `<Device Name>` | Setup | **Physical Ports**. For information the options in this page, see the **IPS Administration Guide** or the **Online Help**.

**Rule Objects**

Note the following changes:
In Manager 8.2, you can manage all types of rule objects in the Rule Objects page (Intrusion Prevention | Objects | Rule Objects). The Rule Objects page is available only under Objects.

You can also dynamically create and edit rule objects from the relevant features. However, dynamic creation is limited to only the applicable rule objects types. For example, in the Firewall policies, you cannot create service range rule object.

For information on how to use the Rule Objects page, see the Network Security Platform 8.2 IPS Administration Guide.

Rule Objects in the Central Manager
From release 8.2.7.4x, rule objects are available in the Central Manager. To know more about the rule objects feature in the Central Manager, see the latest Network Security Platform 8.2 Manager Administration Guide.

On policy synchronization, the Central Manager sends the rule objects only to those Managers, which are on 8.2.7.4x and later.

Attack Set Profiles (formerly, Rule Sets)
Rule Sets is renamed to Attack Set Profiles. So, options and page names are all renamed accordingly. To access Attack Set Profiles page, select Policy | <Admin Domain Name> | Intrusion Prevention | Objects | Attack Set Profiles.

To include only McAfee Recommended For SmartBlocking (RfSB) attacks in an attack set profile, select RfSB only from the Attack Type drop-down in the Details section of Attacks to Include / Exclude tab.

Take note if you have a heterogeneous Manager environment managed by an 8.2 Central Manager. During policy synchronization, the attack set profiles from the Central Manager are created as rule sets in the pre-8.2 Managers.

IPS Policies
This section applies to both Central Manager and Manager. The IPS policy configurations are preserved during the upgrade.

You can rename IPS policies except the default ones.

Reconnaissance attack definitions are available in the IPS policies.

In the IPS policies, reconnaissance attack definitions are categorized as reconnaissance signature attack and reconnaissance correlation attack.

In the IPS policies, the applications relevant to attack definitions are not displayed.

Sorting, grouping, and filtering options for attack definitions are changed.

Because reconnaissance policies deprecated, the IPS policies in Manager 8.2 include the default reconnaissance attack definitions. However, when you do a configuration and signature set update, the Manager deploys the reconnaissance attack definitions in the IPS policies only on the 8.2 Sensors.

In Central Manager and Manager 8.2, the Default IPS Attack Settings is available in the IPS Policies page.

For detailed information on the IPS Policies page and how to manage IPS policies in Manager 8.2, see Network Security Platform 8.2 IPS Administration Guide.

Exception Objects (applies to Sensors and NTBA Appliances)
Exception Objects in version 8.1, 8.0, and 7.5 is referred as Attack Filters in version 7.1. In a homogeneous 8.2 Sensor environment, Exception Objects is replaced by Ignore Rules.
Ignore Rules is a rule-based advancement of Exception Objects. The other highlights of Ignore Rules are:

- You can use dynamically created rule objects in Ignore Rules.
- Centralized assignment is possible. That is, you can set a device, interface, or subinterface as the scope for an ignore rule from the same page.

Notes:

- After you upgrade the Manager and Sensors to 8.2, the attack filters and exception objects, which are assigned to attack definitions are automatically converted into ignore rules. Also, Manager 8.2 applies these ignore rules to the corresponding attack definitions at domain, Sensor, and interface levels. In short, exception-object configuration and assignment are preserved during the upgrade without user-intervention.

The exception objects, which are not assigned to any attack definitions are lost during upgrade.

- When you upgrade the Manager, ignore rules are created for those exception objects, which are created at the domain level and assigned to attack definitions. If the exception objects configuration is different for inbound and outbound, different ignore rules are created for inbound and outbound. However, until you upgrade the Sensors also to 8.2, you must use the Exception Objects page to manage exceptions.

- When you upgrade a Sensor to 8.2, the Manager converts the corresponding exception objects at the Sensor and interface levels (of that Sensor) into ignore rules. From now on, you use the Ignore Rules page for the upgraded Sensor.

- Notes on how the exception objects from earlier releases are named when converted into ignore rules post-upgrade:
  - In exception objects, you can specify multiple one-to-one matching criteria. For example, the exception object is applied only if any of the following criteria matches:
    - Source IP address is 10.10.10.10 and destination IP address is 11.11.11.11.
    - Source IP address is 20.20.20.20 and destination IP address is 21.21.21.21.
  
  In the same ignore rule, you cannot define multiple one-to-one matching criteria. To create the equivalent ignore rule for the above example, you must create different ignore rules for each matching criteria.

  - The exception objects at admin domain are named based on the following convention: <exception object name>_ <internal domain ID>_ <attack definition direction>_ <matching criteria ID>. Consider that you created an exception object example in the domain My Company and assigned to an attack definition in the outbound direction. Post-upgrade, this exception object is converted to an ignore rule named example_0_Out_0. The ignore rule is named example_0_In_0 if applied on an inbound attack definition. If the same exception object is applied in both inbound and outbound, only one ignore rule is created. This ignore rule is named as example_0_Both_0. If the exception object is applied on a reconnaissance attack definition, the ignore rule is named as example_0_Recon_0. In case of NTBA, the ignore rule is named as example_0_Ntba_0.

  - The convention for exception objects created at device level is: <exception object name>_ <internal domain ID>_ <internal device ID>_ <attack definition direction>_ <matching criteria ID>. For example, the ignore rule is named as example_0_1001_Both_0. In the case of NTBA, the ignore rule is named as example_0_1002_Ntba_0.
The convention for exception objects defined at interface level is: `<exception object name>_<internal domain ID>_<internal device ID>_<internal interface ID>_<attack definition direction>_<matching criteria ID>`. For example, `example_0_1001_101_Both_0`.

Post-upgrade, the Manager creates a rule object for every source and destination criteria values if the type is IP address or IP address range. Consider that you specify 10.10.10.10 as the source matching criteria in an exception object. During upgrade, the Manager checks if there is any available rule object for IP address 10.10.10.10 within the same domain. If available, that rule object is used in the ignore rule. If not, the Manager creates a rule object for IP address 10.10.10.10 and uses this rule object as the source matching criteria in the ignore rule.

In a heterogeneous Sensor environment, you use the **Exception Objects** page for the pre-8.2 Sensors and **Ignore Rules** for the 8.2 Sensors.

In the Real-time Threat Analyzer, for the alerts raised by the pre-8.2 Sensors, you use the **Create New Exception** right-click option. This functionality is the same as in the earlier releases. For the alerts raised by 8.2 Sensors, you use the **Create Ignore Rule** right-click option. For the alerts raised by 8.2 Sensors, you cannot apply an existing ignore rule but apply only a new ignore rule.

In 8.2, to create an ignore rule at the domain level, do not select any resource for **Scope**. For such rules, the **Scope** field in the ignore rule is indicated by a dotted line. So, such rules are applied to all Sensor resources owned by the corresponding admin domain. Also, such admin-domain ignore rules are automatically inherited by child domains and applied to the Sensor resources owned by the child domains as well.

After you upgrade all Sensors to 8.2, review the ignore rules created during the upgrade to further optimize them.

When there are no pre-8.2 Sensors, **Exception Objects** and **Assignments** are removed automatically from the Manager user interfaces.

**Navigation path to Ignore Rules page in Manager 8.2:** Policy | `<domain name>` | Intrusion Prevention | Exceptions | Ignore Rules.

**Navigation path to Exception Objects page in Manager 8.2** (This page is displayed only if there are pre-8.2 Sensors): Policy | `<domain name>` | Intrusion Prevention | Exceptions | Exception Objects.

The **Assignments** page applies to exception objects and not to ignore rules. Therefore, the **Assignments** page is available only if there are pre-8.2 Sensors. You can assign ignore rules to attack definitions from the **Ignore Rules** page.

**Exception Objects in the Central Manager:**

From release 8.2.7.4x, you can define ignore rules in the Central Manager.

In the earlier versions, you had to create exception objects in the Exception Objects page and associate them with attacks through the Assignments page.

The notes on exception objects and ignore rules, mentioned above for Managers, apply to a Central Manager as well. The following are some additional notes you must consider for a Central Manager.

- In a heterogeneous Manager environment, you use the **Exception Objects** page for the pre-8.2 Managers and **Ignore Rules** page for the 8.2 Managers.

- Even if there are no pre-8.2 Sensors in your deployment, **Exception Objects** and **Assignments** pages are available in Central Manager 8.2. During the synchronization process, the Central Manager sends the exception objects and assignments to all Managers and this data persists in the Manager database. However, the Managers display the **Exception Objects** and **Assignments** pages only when there are pre-8.2 Sensors.
In the earlier versions, you had to create exception objects in the Exception Objects page and associate them with attacks through the Assignments page. Now, the Ignore Rules page gives you the convenience of linking ignore rules with attacks within the same page, i.e. the Ignore Rules page. There are two scenarios to consider here. You can either create ignore rules from the Ignore Rules page or you can automatically upgrade exception objects to ignore rules during a version upgrade. The second option is important when you are upgrading Central Manager from a pre-8.2 version. When you upgrade Central Manager to 8.2 from a previous version, these exception objects appear—after conversion—as a set of ignore rules in the Ignore Rules page.

When you upgrade the Central Manager to 8.2.7.4x and later, the exception objects assigned to attacks in the Central Manager are converted to ignore rules. These exception objects are also preserved during the upgrade of the Central Manager.

The exception objects not assigned to any attacks are not converted to ignore rules.

The exception objects assigned to attacks in the Central Manager are not converted into ignore rules when you upgrade the Manager to 8.2.7.4x and later. However, exception objects defined in the Central Manager but assigned to attacks in the Manager are converted into ignore rules when you upgrade the Manager. These ignore rules are owned by the Manager.

In the initial version of 8.2, ignore rules feature is introduced only in the Manager and not available in the Central Manager. In release 8.2.7.4x, ignore rules is introduced in Central Manager as well. If you upgrade from the initial version of 8.2 to 8.2.7.4x and later, some of the ignore rules might be duplicated in the Central Manager and Manager. To avoid sending duplicate ignore rules to the Sensor, the ignore rules created during the Central Manager upgrade are disabled by default. You can change it to "enabled" state later if you wish so. This applies only when you upgrade from an initial 8.2 version to 8.2.7.4x and later.

After you upgrade the Manager, delete any duplicate ignore rules in the Managers and enable the corresponding ignore rules in the Central Manager. So, during the next policy synchronization, these ignore rules are available at the Managers.

For any upgrade that happens from 7.1, 7.5 or 8.1 to 8.2, the upgraded ignore rules will appear as "enabled." The automatic upgrade converts all pre-existing exception objects (that are already associated with attacks through the Assignments page) to ignore rules.

The naming convention for exception objects created in Central Manager is: <exception object name>_<domain>_<direction of attack>. For example, a name would appear as example_0_in/out/both. The domain will always remain "0" in case of Central Manager.

To create ignore rules, see Chapter How to create Ignore Rules for an applied IPS policy in Network Security Platform IPS Administration Guide.

Protection Profile and Protection Options

From release 8.2, the Protection Profile feature is deprecated. This feature is replaced by a new feature called Policy Manager. The Policy Manager is an advancement of the Protection Profile feature. From the Policy Manager, you can create, edit, and assign policies to Sensors and Sensor interfaces/subinterfaces. So, post-upgrade you use the Policy Manager instead of Protection Profile. The main advantage of the policy manager is that you can create, edit, and assign the security policies for a specific interface or subinterface from the same page. You can also now view the policy assignments of all devices in a domain from the same page.

Because Protection Profile is deprecated, Protection Options is also deprecated. Protection Options feature is now available through a policy called the Inspection Options policy. A corresponding inspection option policy is automatically created with your pre-8.2 configuration and applied to the corresponding interfaces and subinterfaces.

What happens to your earlier configuration through Protection Profile and Protection Options?
When you upgrade the Manager, all your earlier Protection Profile and Protection Options settings are preserved.

When you upgrade a Sensor to 8.2, the pre-8.2 policies you applied through Protection Profile are still applied. Similarly, the Protection Options are also applied now as inspection option policies. So, your network is protected according to your earlier configuration even after the upgrade without you having to intervene. The exceptions to this are the customized reconnaissance attack definitions. Recall that from release 8.2, reconnaissance policies are deprecated, and you must manually merge your reconnaissance policy with the required IPS policies post upgrade.

**How the Inspection Option Policies are created for pre-8.2 Protection Options configuration?**

Based on the protection options applied to an interface or subinterface, an inspection option policy is created. This policy is named using the following convention: Inspection Options Policy

<admin-domain-name> <Sensor-name> <interface-name>/<subinterface-name>

This policy is applied to the corresponding interface or subinterface. If there are any other interface or subinterface within the same domain and with the same protection option configuration, then this policy is applied to those interfaces and subinterfaces as well. Similarly, the Manager creates an inspection option policy for every unique set of protection options within the same domain. The Manager also automatically applies these inspection option policies to the corresponding Sensor resource.

If the protection options were same for interfaces even across Sensors (but within the same domain), the same inspection options policy is applied. For example, Sensor-A and Sensor-B belong to a domain called, *My Company*. Ports 1A-1B and 4A-4B of Sensor-A and 2A-2B of Sensor-B have the same protection options before upgrade. During upgrade, the Manager creates an inspection option policy named *My Company Sensor-A 1A-1B*, and applies this policy to ports 1A-1B and 4A-4B of Sensor-A as well as 2A-2B of Sensor-B. Post upgrade, if necessary, you can clone this policy, rename the cloned policies, and apply to the respective interfaces and subinterfaces.

To manage the inspection option policies post-upgrade, see *Network Security Platform 8.2 IPS Administration Guide*.

**Notes:**

- In Manager 8.2, because the protection options are part of inspection option policy, inheriting the domain-level Default Device Settings at an interface or subinterface is not supported. When you upgrade, the inspection option policies are created based on the settings applied to interfaces and subinterfaces.

- The domain-level Default Device Settings settings are not migrated if the corresponding protection option is not enabled prior to upgrade. However, any configuration at the interface or subinterface are migrated even if the corresponding protection option is not enabled prior to upgrade.

  In short, all configuration at the interface or subinterface level is migrated regardless of whether the protection option is enabled.

- Heterogeneous Sensor environment — In the previous releases, the unsupported protection options are grayed out for Sensors on earlier versions. However in Manager 8.2, an unsupported feature is not indicated in the user interface. But, during a configuration update, the Manager sends only the applicable settings to the Sensors on lower software versions.

- The inspection option policies contain the Legacy Malware Detection tab if the Manager detects any Sensors on 7.1 software. See *Note regarding File Reputation (Artemis)* on page 154.

The following table captures the differences between using Protection Profile in the earlier releases and Policy Manager in 8.2:
<table>
<thead>
<tr>
<th>Task</th>
<th>Protection Profile in earlier releases</th>
<th>Policy Manager in release 8.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign an IPS policy to a device.</td>
<td>Devices</td>
<td>admin domain name&gt;</td>
</tr>
<tr>
<td>Assign a reconnaissance policy to a device.</td>
<td>Same navigation path as above.</td>
<td>• 8.2 Sensors: Not available. Recall that from release 8.2, reconnaissance policies are deprecated and the reconnaissance attack definitions are part of IPS policies. See Inclusion of reconnaissance correlation attack definitions in IPS policies on page 165. • Pre-8.2 Sensors: To view the assigned policy or assign a different reconnaissance policy, select Policy</td>
</tr>
<tr>
<td>Assign the device-level Firewall policy</td>
<td>Same navigation path as above.</td>
<td>Select Policy</td>
</tr>
<tr>
<td>Device-level protection options: Enabling Simulated Blocking.</td>
<td>Same navigation path as above.</td>
<td>Select Devices</td>
</tr>
<tr>
<td>Assigning the following policies in the protection profile of interfaces and subinterfaces:</td>
<td>Devices</td>
<td>&lt;admin domain name&gt;</td>
</tr>
<tr>
<td>• Baseline IPS policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Customize the baseline IPS policy to create a local IPS policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Advanced malware policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Firewall policy at port and interface or subinterface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Connection limiting policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• QoS policy (at interface level only)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Protection Profile in earlier releases</td>
<td>Policy Manager in release 8.2</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------</td>
<td>-------------------------------</td>
</tr>
</tbody>
</table>
| Configuring the following protection options settings for interfaces and subinterfaces (the old names are in brackets):  
  • Advanced Botnet Detection  
  • Traffic Inspection (Advanced Traffic Inspection) | Same navigation path as above. | Use the inspection option policies (Policy | <admin domain name> | Intrusion Prevention | Inspection Option Policies). There are separate subtabs within the inspection options policy. You can apply different inspection option policies to different interfaces and subinterfaces.  
  In addition to all options of Advanced Traffic Inspection of the earlier releases, Traffic Inspection in 8.2 contains the following as well:  
  • HTTP Response Traffic Scanning  
  • X-Forwarded-For (XFF) Header Parsing  
  • Layer 7 Data Collection  
  • Passive Device Profiling  
  • Attack Blocking Simulation (Simulated Blocking) |
<p>| - Web Server - Heuristic Analysis (Heuristic Web Application Server Protection) | | |
| - Web Server - Denial of Service Prevention (Web Server - Denial of Service Protection) | | |</p>
<table>
<thead>
<tr>
<th>Task</th>
<th>Protection Profile in earlier releases</th>
<th>Policy Manager in release 8.2</th>
</tr>
</thead>
</table>
| Enabling the following features for interfaces and subinterfaces:  
- HTTP Response Scanning  
- Layer 7 Data Collection  
- Passive Device Profiling  
- Attack Blocking Simulation (Simulated Blocking)  
- X-Forwarded-For (XFF) Header Parsing | Same navigation path as above. To configure these settings, click the feature name, which displays a pop-up. | You can enable these features in the Traffic Inspection tab of inspection option policies. To configure the settings for these features, select Devices | admin domain name | Devices | device name | Setup | Advanced. |

HTTP Response Scanning and X-Forwarded-For (XFF) Header Parsing have no configuration settings.

<table>
<thead>
<tr>
<th>Endpoint Reputation Analysis (IP Reputation)</th>
<th>To enable IP Reputation, select Devices</th>
<th>admin domain name</th>
<th>Devices</th>
<th>device name</th>
<th>IPS Interfaces</th>
<th>interface or subinterface name</th>
<th>Protection Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>To configure IP Reputation, select Devices</td>
<td>Global</td>
<td>Default Device Settings</td>
<td>IPS Devices</td>
<td>IP Reputation.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

You can enable and configure Endpoint Reputation Analysis in the Endpoint Reputation Analysis tab of inspection option policies.

- Regarding Endpoint Reputation Analysis, what is referred by IP address is now referred as endpoint. So, the option names are also renamed accordingly.
- In the policies of 8.2 Manager, inheritance of configuration is removed. So, the Inherit CIDR Exclusion list from GTI Participation Page option is deprecated. This does not impact the upgrade process.
- From release 8.2, you must maintain the CIDR exclusions separately for GTI Participation Page from the CIDR exclusions of Advanced Botnet and Endpoint Reputation Analysis.

**Note on IPS signature sets and botnet detectors**

From 8.2, IPS Signature Sets is renamed as Signature Sets; Botnet Detectors is renamed as Callback Detectors. Because of these terminology changes, the related options and page names in the Manager are also renamed accordingly.

**Note on whitelisted and blacklisted file hashes**

The whitelisted and blacklisted file hashes, which you configured in your current version are preserved during the upgrade. In Manager 8.2, the Whitelisted and Blacklisted Hashes page is available at Policy | root admin domain name | Intrusion Prevention | Exceptions | File Hash Exceptions.
Notes regarding Advanced Malware Policies

- In this release, the NTBA malware engine is renamed as Gateway Anti-Malware engine. In the Advanced Malware policies, if you select NTBA prior to upgrade, post-upgrade the Gateway Anti-Malware engine is selected.

- Earlier NTBA and Advanced Threat Defense appliances had a built-in Gateway Anti-Malware Engine. Now, NS-series Sensors on 8.2 also have a built-in Gateway Anti-Malware Engine.

Scenario 1: NS-series Sensors and NTBA are deployed. If the Sensor is on a pre-8.2 version, the Sensor sends the supported files to NTBA for Gateway Anti-Malware Engine scanning. After you upgrade the NS-series Sensor to 8.2, the Sensor sends the files to its built-in Gateway Anti-Malware Engine instead of NTBA.

Scenario 2: M-series and Virtual IPS Sensors with NTBA deployed. As in the earlier version, a Sensor on 8.2 version, sends the supported files to NTBA for Gateway Anti-Malware Engine scanning.

In the above example, you apply the same Advanced Malware policy to all the Sensors. However, the Gateway Anti-Malware Engine functionality automatically varies based on the model and software version of the Sensors.

- In earlier releases, the Sensor first checks a file against the whitelist and blacklist. If there is no match, the Sensor submits the file to all the configured malware engines simultaneously. In version 8.2, the malware analysis sequence is based on the Sensor model:

- In release 8.2, if any of the other malware engines report the malware confidence as medium or above for a file, the Sensor does not submit that file to Advanced Threat Defense for dynamic analysis. The objective is to send only unknown files to Advanced Threat Defense for dynamic analysis.

For information on the enhancements to the Advanced Malware policies in this release, see the Network Security Platform IPS Administration Guide and the Network Security Platform 8.2 Release Notes.

Note on Quarantine

- In the 8.2 Manager, the navigation path to customize quarantine browser message is as follows:
  Devices | <domain_name> | Global | IPS Device Settings | Quarantine | Browser Messages

- In the 8.2 Manager, the navigation path to configure Remediation Portal settings is as follows:
  Devices | <domain_name> | Global | IPS Device Settings | Quarantine | Remediation Portal

- The Summary page to view the quarantine summary for an admin domain is deprecated in the 8.2 Manager.

Note regarding custom attacks

This note is relevant only if you use McAfee custom attacks or Snort custom attacks.

McAfee custom attack verification: McAfee custom attacks (including the McAfee-supplied ones) created in the earlier Manager are test compiled during upgrade to ensure there are no incompatibilities with the current McAfee signature set. If any such incompatibilities exist, a fault is raised, which is visible in the System Faults page. If you encounter problems with a particular McAfee custom attack, you need to recreate it.

Notes regarding Snort custom attacks
If you have Snort custom attacks in version 7.x, then you must re-submit them for translation after you upgrade the Manager to 8.x. See Resubmit Snort custom attacks for translation on page 184.

After you upgrade to Network Security Platform 8.2, signature set update for Sensors could fail because of Snort custom attacks that contain unsupported PCRE constructs. In such cases, the Incompatible custom attack fault is raised in the System Faults page. Check your Snort custom attacks for any of the constructs listed below. If the rules contain any of these unsupported constructs, you either have to delete them from the Snort Custom Attacks or create equivalent rules that do not use these constructs. The following are the unsupported constructs:

- Lookahead and lookbehind assertions.
- Backreferences and capturing subexpressions.
- Subroutine references and recursive patterns.
- Conditional patterns.
- Unicode character properties \p{xx} and \P{xx}.
- Possessive quantifiers.

Note regarding McAfee® ePolicy Orchestrator®

The Network Security Platform extension running on McAfee ePO must be compatible with your current version of Network Security Platform. Consider that you integrated McAfee ePO with the earlier version of Network Security Platform, and then subsequently you upgraded Network Security Platform. Then the integration with McAfee ePO might not work as expected because the Network Security Platform extension on McAfee ePO is from an old installation. This extension might not be compatible with your current version of Network Security Platform. To verify this, you can use the Test Connection button in step 2 of the ePO Configuration Wizard in your current Manager. If the Network Security Platform extension is incompatible, an error message is displayed along with the minimum required version for the extension.

To integrate with Network Security Platform 8.2, you need McAfee ePO 4.6 or 5.1.
Notes regarding McAfee® Vulnerability Manager

Prerequisite for the integration to succeed

Disabling CBC protection allows the integration. Cipher block chain (CBC) protection is an operating mode in cryptography. Java uses CBC protection in SSL connections to counter the Beast Exploit against SSL/TLS (BEAST) threat, and a security vulnerability in an SSL socketFactory method. This security fix was introduced in Java version 6u29, which also introduced a bug that prevents SSL connections to SQL Server 2008. As a result, CBC protection interferes in the integration between the Manager and MS SQL database of Vulnerability Manager. Therefore, before you proceed with your configuration of Vulnerability Manager in the Manager, disable this feature by performing the steps below:

1. Locate the `tms.bat` file in `C:\Program Files\McAfee\Network Security Manager\App\bin`.
2. Open the file in a notepad application.

```bash
rem This section is for configuring the Java environment
rem
set JAVA_OPTS=%JAVA_OPTS% -Djsse.enableCBCProtection=false
rem
set JAVA_OPTS=%JAVA_OPTS% -Djava.security.egd=file:///dev/urandom
```
3. Scroll to locate the text displayed in the image as (1).
4. Once you have located the text, append it with the following entry:
   ```bash
   set JAVA_OPTS=%JAVA_OPTS% -Djsse.enableCBCProtection=false.
   ```
   The text must be entered as displayed in the image as (2).
5. Save and close the file.
6. Re-start the Manager.
   Once the Manager is back up you may proceed with the configuration.

Upgrade paths

You can integrate only the following McAfee Vulnerability Manager versions with Manager 8.1:

- McAfee Vulnerability Manager 7.0
- McAfee Vulnerability Manager 7.5
Note regarding Network Security Platform and McAfee Logon Collector integration

Network Security Platform 8.2 integrates only with McAfee® Logon Collector 2.1 and later. Therefore, if you had integrated Network Security Platform and McAfee Logon Collector prior to upgrade, make sure that the version of Logon Collector is 2.1 or later for this integration to work with Network Security Platform 8.2.

NTBA-related enhancements from release 8.2

Network Forensics configuration

From release 8.2, NTBA supports context-aware network forensics to capture connections and layer 7 activity before and after a security event. This helps forensic analysis to be performed on the contextual data, against a set of predefined indicators.

In the earlier releases, you can enable Network Forensics only for one NTBA device (per Manager) at a given time. In 8.2, you can enable Network Forensics for all your NTBA devices. Also, in 8.2 there are now more options to configure network forensics. Based on the enhancements in Network Forensics, the user interfaces and functionality of the feature are also correspondingly enhanced.

Given the extensive enhancements in Network Forensics, your network forensics configuration prior to upgrade is lost. Assume that you enabled network forensics for one of your NTBA devices prior to upgrade. When you upgrade the Manager to 8.2, the previous network forensics feature configuration is lost. Also, you cannot enable or configure network forensics feature until you upgrade the NTBA device.

NTBA storage infrastructure is enhanced such that context data is available for a longer duration. Because of these enhancements, you might experience NetFlow data to be stored for a lesser duration when your network traffic is very high.

In 8.2, the network forensics feature is available in the Collection Settings page. The Network Forensics page (Manage | <Domain name> | Integration | Network Forensics) in 8.1 is removed. For more information on network forensics enhancements and the navigation path to the Collection Settings page, see the Network Security Platform 8.2 NTBA Administration Guide.

Netflow Exporter configuration enhancement

Earlier, once you configured the Sensor or router to export NetFlows to an NTBA Appliance, you had to define the interfaces in a separate step. With the 8.2 release, you can define an exporter and interface details in a single step. This helps to define an exporter end-to-end and check port connectivity immediately.

From the Manager, go to Devices | <Domain name> | Devices | <NTBA Appliance> | Exporters | Exporters to define an exporter and its interfaces. Alternatively, define a Sensor exporter by navigating to Devices | <Domain name> | Devices | <Sensor> | Setup | NTBA Integration.

Exception objects enhancements (Ignore rules)

See Performance and usability enhancements in Manager 8.2 on page 166 for enhancements regarding exception objects.
**Gateway Anti-Malware updates**

- Your Gateway Anti-Malware Engine update settings are maintained during the upgrade.
- The **Gateway Anti-Malware Engine Updating** page in the earlier releases is deprecated (Devices | <domain name> | Global | Default Device Settings | NTBA Devices | NTBA Device Settings | Maintenance | Gateway Anti-Malware Engine Updating). In Manager 8.2, use the **GAM Updating** page at Devices | <domain name> | Global | Common Device Settings | GAM Updating).

**NTBA CLI enhancements**

- The **show exporters** command has been enhanced to display the interface count.
- The **show dbstats** command is improved for readability.
- The flow forwarding commands **flowforward collector** and **show flowforwardinfo** are reintroduced to define and view flow forward collectors details.

**Backing up Network Security Platform data**

Before you upgrade, back up your tables and save any McAfee custom attacks (formerly UDS) that you have created. If you have a very large number of alerts and packet logs to upgrade, first consider archiving and deleting any alert and packet log data that you do not need before creating your database backup files.

![Save your entire backup in a different location than the current Central Manager or Manager to prevent data loss.](image)

After you back up the Network Security Platform data, you can consider purging the Manager tables. Details on how to purge the database tables are in the *Network Security Platform Manager Administration Guide*.

Purging the database tables can significantly shorten the Manager upgrade window. If you need the older alerts and packet logs, you can restore the database backup on an offline Manager server for viewing and reporting on that data.

**Perform a database backup**

Back up your database before you upgrade. McAfee strongly recommends the following.

- All tables backup
- Config tables backup
- Archiving alerts and packet logs

All tables backup is time consuming (based upon the size of your database); however, it guarantees the integrity of your existing data. All tables backup includes the entire database, that is, all configurations, user activity, alert information, and custom attacks. However, McAfee recommends a separate all tables and config tables backup. This provides you options if for some reason you want to roll back to your earlier version of the Central Manager or Manager.

**Notes:**

- Preferably, stop the Central Manager or Manager service before you begin any backup process.
- For step-by-step information on all tables and config tables backup as well as archiving alerts and packet logs, see the *McAfee Network Security Platform Manager Administration Guide*. 
Back up McAfee custom attacks

If you have McAfee custom attacks, back them up prior to upgrade. Refer to the corresponding version of the *McAfee Network Security Platform Custom Attacks Guide* for information on how to back up custom attacks from the Central Manager and Manager.

---

**Operating system upgrade scenarios**

In this section, the term *Manager* refers to both Central Manager and the Manager.

The following sections discuss some possible scenarios that involve an operating-system upgrade for your Manager. These are based on your current Manager version, operating system, and whether you want to migrate the Manager server to a new physical system.

For information on how to upgrade the operating system, refer to Microsoft’s documentation.

**Manager and operating system upgrade**

You can install 7.1, and 7.5 Manager server on Windows Server 2008 R2 (Standard or Enterprise Edition) English/Japanese (64 bit). The 8.2 Manager is supported on various flavors of Windows Server 2012 as mentioned in *Central Manager and Manager system requirements* on page 140.

If you plan to upgrade the operating system to a supported flavor of Windows Server 2012, you can consider the approaches discussed in the subsequent sections.

**Tasks**

- **Approach 1: Upgrade the operating system and the Manager** on page 180
- **Approach 2: Using new hardware** on page 181

**Approach 1: Upgrade the operating system and the Manager**

**Before you begin**

- It is assumed that your 7.x Manager server is on Windows Server 2008 R2 Standard or Enterprise Edition, SP1, English or Japanese (64 bit) (Full Installation).

- It is assumed that the 7.x Manager meets the minimum requirement to upgrade to 8.x. If not, first upgrade the Manager to the required 7.x version.

- It is assumed that your 7.x Manager server meets the requirements for the corresponding English or Japanese versions of Windows Server 2012.

- Note that a typical operating system upgrade can take around an hour. So the Manager upgrade downtime window would extend by that much.

**Task**

1. Back up the 7.x database.
   
   See *Backing up Network Security Platform data* on page 142.

2. Upgrade the Manager to the 8.x version.
   
   See *MDR Manager upgrade* on page 182 or *Standalone Manager upgrade* on page 183 as per your deployment. In case of Central Manager, see *MDR Central Manager upgrade* on page 143 or *Standalone Central Manager upgrade* on page 144.
3. Log on to the Manager and check the Status page to ensure everything is working fine.

   For MDR, complete these steps this procedure for one of the Manager and then proceed to the other.

4. Upgrade the operating system to English or Japanese version of the corresponding Windows Server 2012.

5. Log on to the Manager and check the Status page to ensure everything is working fine.
   If everything is working fine, it means that the upgrade was successful.

6. Back up the 8.x Manager database.
   This backup is the baseline of your 8.x Manager.

**Approach 2: Using new hardware**

**Before you begin**

- It is assumed that you have a system installed with the required Windows Server 2012 flavor.
- It is assumed that this system meets the other requirements discussed in Upgrade requirements for the Manager on page 147.
- It is assumed that the 7.x Manager version meets the requirement to upgrade to 8.x. If not, first upgrade the Manager to the required 7.x version.

**Task**

1. Back up the 7.x database.
   See Backing up Network Security Platform data on page 142.

2. Upgrade the Manager to the latest 8.x version.
   See MDR Manager upgrade on page 182 or Standalone Manager upgrade on page 183 according to your deployment. If Central Manager, see MDR Central Manager upgrade on page 143 or Standalone Central Manager upgrade on page 144.

3. Back up the 8.x Manager database.

4. On the new Windows Server 2012 server, install the same version of 8.x Manager as in step-2.

5. On the network, replace the existing 8.x Manager server with the new 8.x Manager.
   Make sure that the IP address of the new Manager is the same as that of the existing one. If the IP address is different, the Sensors cannot communicate with the new Manager system. In that case, re-establish this communication from each Sensor.

6. Restore the 8.x database backup from the old 8.x Manager on the new 8.x Manager.
   For information on how to restore a database, see the latest Manager Admin Guide.

7. Log on to the new 8.x Manager and check the Status page to make sure everything is working fine.

8. Back up the 8.x database of the Manager server.
   See Perform a database backup on page 143.

   In case of MDR, complete this procedure fully for one Manager before you proceed to the next.
MDR Manager upgrade

Before you begin
Make sure both the Managers meet the required system requirements as mentioned in Central Manager and Manager system requirements on page 140.

This section provides the steps to upgrade the primary and secondary Managers configured for Manager Disaster Recovery (MDR).

Task

1. Using the Switch Over feature, make the secondary Manager active.
   - If your current Manager version is earlier than 7.5, select My Company | Manager | MDR | Manager Pair | Switch Over.
   - For 7.5 and later, click Manage and select the root admin domain. Then go to Setup | MDR | Switch Over.

2. Upgrade the primary Manager to 8.2.
   For information, see Standalone Manager upgrade on page 183.

3. Bring up the upgraded primary Manager.
   The primary is up in standby mode.

4. Stop the secondary Manager.
   Because the versions of the primary and secondary Manager are now different, you must stop the secondary; else you cannot complete the next step.

5. Using the Switch Back feature, make the primary the active Manager.

6. Upgrade the secondary Manager to 8.2.

7. Bring up the upgraded secondary Manager.
   The secondary is up in standby mode. Make sure the latest 8.7 signature set is present in both the Managers.

Differences in alerts displayed by the Managers

When you upgrade an MDR pair, the Manager currently being upgraded could miss the alerts during the upgrade window. However, its peer receives these alerts. After you successfully upgrade both the Managers, the missed alerts are updated for both the Managers during the next automatic synchronization. Note that the Managers synchronize every 10 minutes. Therefore, within 10 minutes after you upgraded the MDR pair, the alerts are synchronized.

If the number of alerts missed by a Manager is less than 10,000, all missed alerts are updated in the Manager’s database. The Real-time Threat Analyzer of both the Managers display the same alerts.

If the number of alerts missed by a Manager is more than 10,000, all missed alerts are updated in the Manager’s database. However, only the latest 10,000 of the missed alerts are displayed in the Real-time Threat Analyzer of this Manager. The remaining missed alerts are displayed in the Historical Threat Analyzer. Consider a Manager missed 12,000 alerts during the upgrade. After the synchronization, the latest 10,000 of the missed alerts are displayed in the Real-time Threat Analyzer. The older 2000 missed alerts are displayed in the Historical Threat Analyzer.
Standalone Manager upgrade

Before you begin

- If you are using Central Manager, it must be upgraded to 8.2 before you upgrade the Manager.
- Your current Network Security Platform infrastructure meets all the requirements discussed in Upgrade requirements for the Manager on page 147.
- If you want to upgrade the RAM on the Manager server, make sure you do that before you begin the Manager upgrade.
- You have reviewed and understood the implications of the upgrade considerations discussed in Review the upgrade considerations on page 142.
- You have backed up your current Manager data. See Perform a database backup on page 143.
- As a best practice, make sure all the devices are communicating with the Manager and your deployment is working as configured. This ensures that you do not upgrade with any existing issues.
- You have the latest 8.2 Manager installable file at hand. You can download it from the McAfee Update Server. See the Network Security Platform 8.2 Installation Guide.
- You have your Manager MySQL root password available.
- You have stopped all third-party applications such as Security Information and Event Management (SIEM) agents. It is especially important that you stop any such third-party application that communicates with the MySQL database. The Manager cannot upgrade the database if MySQL is actively communicating with another application.

If this is an upgrade of a Manager in an MDR pair, then you should switch it to standby mode before you upgrade. Make sure you are following the steps in MDR Manager upgrade on page 182.

The following are the tasks to upgrade a standalone Manager.

Task

1. Stop the Manager service.
   Right-click on the Manager icon at the bottom-right corner of your server and stop the service. Alternatively, go to Windows Control Panel | Administrative Tools | Services. Then right-click on McAfee Network Security Manager and select Stop.

2. Stop the McAfee Network Security Manager Watchdog service using the same method as described in step 1.

   Make sure the McAfee Network Security Manager Database service remains started.

3. Exit the Manager tray from the Windows Task Bar.

4. Close all open applications.
   If any application is interacting with the Manager, your installation may be unsuccessful.

5. Move any saved report files and alert archives from the server to some other location.
   The reports are saved at <Manager install directory>\REPORTS folder. The alert archives are saved at <Manager install directory>\alertarchival folder.
6 Run the 8.2 Manager executable.
   Install the software as described in the *Network Security Platform 8.2 Installation Guide*.

7 At the end of the upgrade process, you might be required to restart the server. If prompted, it is highly recommended that you restart the server.
   - Select *Yes, restart my system* to restart the server immediately.
   - Select *No, I will restart my system myself* to complete the upgrade process without restarting the server. You can restart the server at a later point in time. Clicking *Done* in the Manager Installation Wizard will start the Manager services.

8 During the upgrade, you might have been prompted to run additional scripts on the Manager server. After the upgrade is complete, run the scripts only if you had been prompted to do so.

   See *Run additional scripts* on page 185.
   
   ![Warning]
   The system prompts you to run the scripts only if there are 1 million or more alerts or endpoint events in your Manager. You should not run the scripts if not prompted.

9 Open the Manager.
   You may be requested to download the required version of Java Runtime Environment (JRE) if the same or higher version is not present already.

10 Log on to the Manager.
   You can verify the version in the Home page.

11 Check the Status page to ensure that the Manager database and the Sensors are up.
   Refer to the following sections and complete those tasks.
   1 If you have Snort custom attacks in the 7.x Manager, you must complete the tasks in *Resubmit Snort custom attacks for translation* on page 184.
   2 If you have one million or more alerts and events in the current Manager database, you must complete the tasks in *Run additional scripts* on page 185.
   3 Make sure the Manager contains the latest 8.7 signature set.
   4 Upgrade the Sensor software with the latest 8.7 signature set. See *How to perform signature set and Sensor software upgrade* on page 5.

**Tasks**
- *Resubmit Snort custom attacks for translation* on page 184
- *Run additional scripts* on page 185

**Resubmit Snort custom attacks for translation**
From release 8.0, Snort custom attacks are translated into a newer McAfee signature format. This is required to support more Snort rule options as well as for performance improvement. However, the Snort custom attacks in this newer format are incompatible with 7.x Sensors. So, to support a heterogeneous Sensor environment, two signatures are created for each Snort custom attack - one for 8.x Sensors and the other for 7.x Sensors.

After you upgrade the Manager from 7.x to 8.x, it is mandatory that you resubmit all Snort custom attacks for translation to the newer McAfee signature format. Then, two signatures are created for those rules.
Task
1  Start the 8.x Manager and log on.
2  Open the Custom Attack Editor. Select Policy | <domain name> | Intrusion Prevention | Advanced | Custom Attacks | Custom Attack Editor.
3  To re-submit the rules, in the Custom Attack Editor, select File | Snort Advanced | View Snort Variables | Re-Submit Rules using Current Variables.

Turn-off signature for 7.x Sensors
The two signatures are created regardless of whether you have a 7.x Sensor in your setup. This is to address scenarios where one might add a 7.x Sensor to an 8.x Manager later. If you do not require the signature for 7.x Sensors, you can turn it off.

Task
1  Locate the ems.properties file. On the Manager server, go to <Manager install directory>\App \config\.
2  In the ems.properties file, uncomment # iv.snortimport.translation.tpuverion.0.support=false.
   That is, change this line to iv.snortimport.translation.tpuverion.0.support=false.
3  Restart the Manager service.

Run additional scripts

Before you begin
Make sure you have the following:

- Administrator rights to the Manager server.
- Manager database name, user name, and password.

When you upgrade to the latest 8.2 Manager, if there are 1 million or more alerts or host events in your current Manager setup, you are prompted to run two SQL scripts as described in this section. These scripts convert those alerts to the new Manager database schema for version 8.2. If it is an upgrade from 7.1 or 7.5 to 8.2 only, you must run a script for Apache Solr after you run the two SQL scripts.

Make sure that you run the three scripts soon after the Manager upgrade is complete. McAfee recommends that you select a relatively idle time to run the scripts to minimize the impact on performance.
When Manager 8.2 starts, all new alerts come into the 8.2 schema tables. Your original alerts and packet logs are still there in the database with a 'tmp_' prefixed to them. You cannot access these old alerts and packet logs until they are manually converted to the new schema and merged back in. This is accomplished by running the following two scripts:

1. Alertproc_offline_1.sql: When you trigger this script, it runs in the background while the newly upgraded Manager is up and running. You do not need to stop the Manager service when running this script. It takes about an hour per every 4-8GB of the original alert and packetlog tables. For example, for a Manager database of 25 GB, it could take between 3–7 hours. The time taken for alertproc_offline_1.sql to complete depends on the Manager RAM, hard disk speed, the activities on the Manager database, number of users logged on to the Manager, reports being generated currently, alerts from the Sensors, maintenance tasks, and so on.

   The quick and easy way to estimate the time needed for this script is to look at the size of the mysql\data\lf directory. Once started, it runs and only returns the MySQL command prompt after it completes.

   After you trigger this script, do not close the window even if you do not see the MySQL command prompt. This process might take some time but completes eventually.

2. Alertproc_offline_2.sql: Run this script when the MySQL command prompt returns after the first script. You must stop the Manager service to run this script. However, this script takes only a few minutes to complete. This script takes the now-converted original alerts and the alerts that came in while the first script was running and merges them together. It does this by renaming the active tables and then renaming the original tables back to what they had been. The script then merges the new alerts into the converted alert tables.

   The merging is because the original tables are large and the new ones are small. It is much faster to merge the small table into the large one. The assumption is that the alert and packetlog tables for the alerts that come into the Manager while the first script was running are much smaller than the tables with the converted alerts. So we merge the smaller table into the larger, which makes it complete the task much faster. When the second script completes, restart the Manager service.

   Run alertproc_offline_1.sql and alertproc_offline_2.sql only if prompted to do so. The system prompts you only when there are 1 million or more, alerts or host events, in the Manager database. If you run these scripts when not prompted, you receive SQL errors. In this case, contact McAfee Technical Support with the details of the message. If you do not run these scripts when prompted, you will not be able to view the alerts in the Threat Analyzer.

Task

1. After a successful upgrade of the Manager to 8.2, check that it is up, Sensors are connected, and alerts are generated.

2. Log on to the Manager server with administrator rights.

3. To run the scripts easily and successfully, it is recommended that you copy the scripts to the MySQL \bin directory and run the scripts from this location.

   Follow these steps to copy the scripts to the MySQL\bin folder.

   a. Go to <Manager install directory>\App\db\mysql\migrate. Example: C:\Program Files \McAfee\Network Security Manager\App\db\mysql\migrate.

   b. Copy the two scripts — Alertproc_offline_1.sql and Alertproc_offline_2.sql to <Manager install directory>\MySQL\bin.

      For example, copy the scripts to C:\Program Files\McAfee\Network Security Manager \MySQL\bin.
4 On the Manager server, log on to MySQL.
   a On the Manager server command prompt, go to `<Manager install directory>\MySQL\bin`
      For example, go to `C:\Program Files\McAfee\Network Security Manager\MySQL\bin`
   b Run the following command: `mysql -u<Database user name> -p<Database password> db_name`
      For example, run `mysql -uroot -proot123 lf`

5 In the MySQL shell (MySQL prompt), run: `source alertproc_offline_1.sql`
   • When `Alertproc_offline_1.sql` executes, it does not display any progress. So, wait until the script completes.
   • When `Alertproc_offline_1.sql` executes, few log messages are displayed at the MySQL prompt.
     The query for the message adding few columns for alert table takes more time based on factors such as the RAM of the Manager server, hard disk speed, activities involving the Manager database, and so on.
   • When you execute `Alertproc_offline_1.sql`, the MySQL prompt drops to the next line and the cursor is restored only when the script is fully executed.
   • If you stop `Alertproc_offline_1.sql` before it executes fully, you might lose the historical alerts and packetlogs. For such cases, revert to the earlier version of the Manager, restore the database backup from prior to upgrade, and then restart the upgrade process.
   • If an SQL error message is displayed, stop proceeding and contact McAfee Technical Support with the details of the message.

6 Stop the Manager service.
   The Manager database service must be running.

7 In the MySQL shell (MySQL prompt), run: `source alertproc_offline_2.sql`
   • `Alertproc_offline_2.sql` typically takes less than a minute to complete.
   • If an SQL error message is displayed, stop proceeding and contact McAfee Technical Support with the details of the message.
   • After you complete running the two scripts, you can delete the two scripts from `<MySQL\bin>` folder since these scripts are might differ between versions.
   • `Alertprocoffline1.log` and `alertprocoffline2.log` files are created in the `<Manager install directory>\App directory`. You can check these logs if there are any issues during the upgrade.
   
   **Utilities like db backup/restore/archival/purge cannot be run on your database before completing step 7. This is because your Manager database will still be in transition at this stage of the upgrade.**
How to Upgrade the Manager?

Standalone Manager upgrade
14 How to perform signature set and Sensor software upgrade

This section contains information on how to upgrade the Sensors to the latest 8.2 version.

Before you proceed with the Sensor software upgrade, you must upgrade the Manager to 8.2.

Contents

- Difference between an update and an upgrade
- Sensor upgrade requirements
- Review the upgrade considerations for Sensors
- Updating Sensor software image

Difference between an update and an upgrade

A software update is a minor release of device software. A device refers to a Sensor or an NTBA appliance as applicable. An upgrade indicates a major release and new feature set. These processes are identical, and thus this section makes references to update and upgrade in an interchangeable manner.

Any change to device software, whether update or upgrade, requires you to do a full reboot of the device.

Sensor upgrade requirements

This section details the requirements to upgrade the Sensor software to 8.2. In this section, the term Sensor refers to M-series, NS-series, and Virtual IPS Sensors unless otherwise specified.

If you are using a hot-fix release, contact McAfee Support for the recommended upgrade path.

Minimum required Sensor software versions
<table>
<thead>
<tr>
<th>Sensor software major release version</th>
<th>Minimum required software versions</th>
</tr>
</thead>
</table>
| 7.1                                   | • M-1250, M-1450, M-2850 and M-2950, M-3050, M-4050, M-6050, M-8000, M-3030, M-4030, M-6030, M-8030, M-8000XC: 7.1.3.119  
  • MS9100, MS9200, MS9300: 7.1.5.72 |
| 7.5                                   | M-1250, M-1450, M-2850 and M-2950, M-3050, M-4050, M-6050, M-8000, M-3030, M-4030, M-6030, M-8000XC: 7.5.3.95 |
| 8.1                                   | • M-1250, M-1450, M-2850 and M-2950, M-3050, M-4050, M-6050, M-8000, M-3030, M-4030, M-6030, M-8000XC: 8.1.3.35  
  • MS9100, MS9200, MS9300: 8.1.5.14  
  • MS7100, MS7200, MS7300: 8.1.5.57  
  • VM-100, VM-600: 8.1.7.14 |
| 8.2                                   | • M-1250, M-1450, M-2850 and M-2950, M-3050, M-4050, M-6050, M-8000, M-3030, M-4030, M-6030, M-8000XC: 8.2.3.12  
  • MS9100, MS9200, MS9300: 8.2.5.11  
  • VM-100, VM-600: 8.2.7.11 |

License file requirement

Physical appliances do not need any licenses.

Review the upgrade considerations for Sensors

Review this section carefully before you commence the upgrade process.

Sensor downtime window

It could take around 15 minutes to upgrade a Sensor. This could vary between deployments. If you have a fail-open setup, to minimize the downtime, perform the following steps, after the Sensor software image is downloaded successfully and before a reboot is initiated:

- If you have gigabit ports connected for fail-open, disable the ports to force fail-open.
- If you have fiber ports configured for fail-open, disable the ports to force fail-open.

Important note regarding M-8000 and M-8000XC Sensor upgrade

It is important that you review this note if you plan to upgrade a Sensor to 8.2 that matches both these conditions:

- It is an M-8000 or an M-8000XC Sensor, which is on a 7.5 software version earlier than 7.5.3.50.
- You plan to upgrade this Sensor using the Manager (and not a TFTP server).

This note does not apply to other Sensor models or M-8000/M-8000XC Sensors on 7.1 software.

When updating a Sensor from the Manager interface, both the Sensor software and the signature set are bundled together and transferred to the Sensor. However, for a Sensor that matches the above conditions, the signature set is not bundled with the Sensor software. Therefore, when the Sensor
reboots after its software upgrade, it deletes the currently loaded signature set, and contacts the
Manager for the latest signature set. (During this time the Sensor’s system health status on the CLI is
displayed as uninitialized.)

Until the Sensor receives the signature set from the Manager, the Sensor cannot process traffic and
raise alerts. Therefore, the Sensor’s downtime is extended by a few more minutes. In other words, the
impact is as if you upgraded the Sensor using a TFTP server though you used the Manager.

As a workaround, you can first upgrade the Sensor to 7.5.3.95 and then upgrade to 8.2.

Note regarding Sensor-NTBA connection
An 8.2 Sensor, for its connections through its management port with NTBA appliances, by default uses
NULL cipher (no encryption). Using NULL cipher is required to support the analysis of much larger
files. If you want this connection to be encrypted, use the following CLI command on the 8.2 Sensor:
set amchannelencryption <on><off>. To know if the connection is currently encrypted, use show
amchannelencryption status on the Sensor CLI.

Enabling encryption can have a performance degradation, which might impact the analysis of large files
and high-volume of files.

IPS CLI changes
From release 8.1, the ARP spoofing CLI command is disabled by default. Post-upgrade to 8.2, the
command is automatically disabled when you reset configuration settings, restore factory defaults, or
add a new Sensor to the Manager.

Updating Sensor software image
Before you begin the Sensor software upgrade, make sure:

1 You have upgraded the Manager to the corresponding 8.2 version.
   See How to Upgrade the Manager? on page 5.

2 Your Sensors meet the requirements mentioned in Sensor upgrade requirements on page 189.

3 You have understood the discussion in Review the upgrade considerations on page 142.

New Sensor software images are released periodically by McAfee and are available on McAfee®
Network Security Platform Update Server to registered support customers.

You can update a Sensor image using any of the four methods illustrated below. These methods
include updating the signature sets as well.

Three of the methods involve updating your image using the Manager server:

1 You can use the Manager interface to download the Sensor image from the Network Security
   Platform Update Server to the Manager server, and then upload the Sensor image to the Sensor.

2 If your Manager server is not connected to the Internet, you can download the Sensor image from
   the Network Security Platform Update Server to any host, then import the Sensor image to the
   Manager server. You can then download the Sensor image to the Sensor.
3 A variation of option 2: you can download the Sensor image from McAfee Network Security Platform Update Server to any host, put it on a disk, take the disk to the Manager server, and then import the image and download it to the Sensor.

4 However, you may prefer not to update Sensor software through the Manager, or you may encounter a situation wherein you cannot do so. An alternative method is to download the software image from the Update Server onto a TFTP server, and then download the image directly to the Sensor using Sensor CLI commands. This process is described in this chapter as well.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>McAfee Update Server</td>
</tr>
<tr>
<td>2</td>
<td>Internet</td>
</tr>
<tr>
<td>3</td>
<td>Manager Server</td>
</tr>
<tr>
<td>4</td>
<td>PC/tftp server</td>
</tr>
<tr>
<td>5</td>
<td>Import/disk</td>
</tr>
<tr>
<td>6</td>
<td>Sensor</td>
</tr>
</tbody>
</table>

**Sensor software upgrade — Manager versus TFTP server**

As indicated in the previous section, the Sensor software can be updated either from the Manager or through a TFTP server. However, if the Sensors are deployed inline in your production network, McAfee recommends updating the Sensor software using the Manager for a major upgrade (for example, from 8.1 to 8.2.)

When updating a Sensor from the Manager interface, both the Sensor software and the signature set are bundled together and transferred to the Sensor. The Sensor updates its Sensor software image, and saves the bundled signature set. When the Sensor is rebooted, it deletes the old Signature Set, and applies the saved signature set that was received along with the Sensor software image.
When updating a Sensor through TFTP, only the Sensor software is transferred to the Sensor. Once the Sensor software update is complete, reboot the Sensor. On reboot, the Sensor deletes the currently loaded signature set, and contacts the Manager for the latest signature set. Until the Sensor receives the signature set from the Manager, the Sensor cannot process traffic and raise alerts.

There will be a Sensor downtime during the Sensor software upgrade process. The downtime is longer in case of an upgrade using TFTP [when compared to using the Manager] due to the additional time required to download the signature set.

Fail-open kits reduce the downtime impact of reboot considerably.

Sensor software and signature set upgrade using Manager 8.2

**Before you begin**
- You have reviewed the notes on Sensor downtime window as well as the important note regarding M-8000 and M-8000XC Sensors. See Review the upgrade considerations for Sensors on page 190.

**Task**

1. If you have not already done so, download the latest 8.7 signature set from the McAfee Network Security Update Server (Update Server).
   - In the Manager, click Manage and select the root admin domain. Then select Updating | Download Signature Sets. See the Manager Administration Guide for step-by-step information on how to download the signature set. For a list of currently supported protocols, see KB61036 at mysupport.mcafee.com. Do not push the signature set to your Sensors at this point; it will be sent with the Sensor software in step 8.

2. If you are using the Advanced Botnet feature, make sure you have downloaded the latest callback detectors to the Manager. See Network Security Platform IPS Administration Guide for the details on downloading callback detectors.

3. Download the most recent 8.2 Sensor software images from the Update Server onto the Manager.
   - a. Click Manage and select the root admin domain. Then select Updating | Download Device Software.
   - b. Select the applicable Sensor software version from the Software Available for Download section and click Download.

4. To push the Sensor software to your Sensors, select Devices | <Domain_Name> | Global | Deploy Device Software.
   - The Deploy Device Software page is displayed.

5. Select the New Version to be downloaded to the Sensor.

*Figure 14-1  Download Software to Devices page*
To select a Sensor for update, select the checkboxes (for the specific Sensor) in the **Upgrade** column.

For the corresponding Sensors, select the checkboxes (for the specific Sensor) in the **Reboot** column.

Click the **Upgrade** button to initiate the process.

**This will push the signature set as well as the software to the Sensors.**

Signature set update could fail because of Snort custom attacks that contain unsupported PCRE constructs. In such cases, the **Incompatible custom attack** fault is raised in the **Status** page. See **Note regarding custom attacks** on page 175.

Wait for the push to complete.

This process takes at least 5 minutes. To know when the process is complete, log on to the Sensor and look for the following status by using the `downloadstatus` CLI command:

- Last Upgrade Status: Good
- Last Update Time: (Time should reflect when the push is complete)

You will be prompted to reboot the Sensor upon completion of the Sensor software upgrade.

Once the reboot process is complete, verify that the Sensor's operational status is up; and that it comes up with the latest software version as well as latest signature set.

- Click the **Devices** tab.
- Select the domain from the **Domain** drop-down list.
- On the left pane, click the **Devices** tab.
- Select the device from the **Device** drop-down list and click **Summary**.
- Use the Threat Analyzer to verify the performance of the Sensors.
  This is to make sure the upgrade was successful. For information on how to check Sensor performance from the Threat Analyzer, see **Manager Administration Guide**.

**If you have a failover pair configured, both the Sensors forming the pair should be running on the same Sensor software version. See **Update Sensor software in a failover pair** on page 195.**

### Sensor software upgrade using a TFTP or SCP server

To download a software image directly to the Sensor through a TFTP or SCP server, you must first download the software image to your TFTP or SCP server. See your TFTP or SCP server documentation for specific instructions on how to download the image to your TFTP or SCP server.

**Task**

1. If you have not already done so, download the latest 8.7 signature set from the McAfee Network Security Update Server (Update Server).

   In the Manager, click **Manage** and select the root admin domain. Then select **Updating | Download Signature Sets**. See the **Manager Administration Guide** for step-by-step information on how to download the signature set. For a list of currently supported protocols, see KB61036 at mysupport.mcafee.com.

   **If you are using the Advanced Botnet feature, make sure you have downloaded the latest callback detectors to the Manager. See **Network Security Platform IPS Administration Guide** for the details on downloading callback detectors.**
2 Download the software image from the Update Server to your TFTP or SCP server. This file is compressed in a .jar file.

3 Rename the .jar file to .zip file.

4 Unzip the file using Winzip.

5 Extract the files to your TFTP boot folder [/tftpboot]. In case of SCP, extract the files to any directory.

6 Once the image is on your TFTP/SCP server, upload the image from the TFTP/SCP server to the Sensor.

   From your Sensor console, perform the following steps:
   a Log on to the Sensor.

      The default user name is **admin** and default password **admin123**.

   b Make sure you have set the TFTP or SCP server IP on the Sensor. Use the `set tftpserver ip` or `set scpserver ip` command as described in the *McAfee Network Security Platform CLI Guide*.

   c Load the image file on the Sensor. Use the `loadimage` command as described in the *McAfee Network Security Platform CLI Guide*.

   d To use the new software image, you must reboot the Sensor. At the prompt, type `reboot`. You must confirm that you want to reboot.

   For some Sensor models, the hitless reboot option is available, wherein only the required software processes are restarted. However, for Sensor software upgrades and updates, you must do a full reboot. For information on these reboot options, see the *McAfee Network Security Platform IPS Administration Guide*.

After the reboot process is complete, the Sensor deletes the old signature set. Because the signature set is incompatible with the current Manager version, the Sensor’s system health status on the CLI is displayed as `uninitialized`. Then, the Sensor contacts the Manager for the latest signature set. After the signature set is downloaded to the Sensor, its system health status is displayed as `good`. Signature set update could fail because of Snort custom attacks that contain unsupported PCRE constructs. In such cases, the **Incompatible custom attack** fault is raised in the **Status** page. See **Note regarding custom attacks** on page 175.

7 Verify the Sensor's system health status is **good**; check the Sensor status from CLI by typing the status command.

   You can also check whether the Sensor is updated with the latest software version as well as latest signature set in the **Summary** page.
   a Click the **Devices** tab.

   b Select the domain from the **Domain** drop-down list.

   c On the left pane, click the **Devices** tab.

   d Select the device from the **Device** drop-down list and click **Summary**.

### Update Sensor software in a failover pair

Because each Sensor in a failover pair must be rebooted after the software update, it is important to update the software in the correct order.
Task

1. Push the software to each of the Sensors that are in the failover pair. You can follow one of these methods:
   - Sensor software and signature set upgrade using Manager 8.2 on page 193
   - Sensor software upgrade using a TFTP or SCP server on page 194.

2. Load the image file on the primary Sensor.

3. Load the image file on the secondary Sensor.

4. Reboot both Sensors concurrently.
   - Use the Threat Analyzer to verify the performance of the Sensors.
     This is to make sure the upgrade was successful. For information on how to check Sensor performance from the Threat Analyzer, see Manager Administration Guide.
Upgrade information for NTBA and XC Cluster

Review this chapter for information on how to upgrade the software for the NTBA and XC Cluster devices.

Contents

- Upgrade NTBA Appliance software
- Upgrade XC Cluster

Upgrade NTBA Appliance software

Before you begin:

- Make sure that you have upgraded the Manager to 8.2. See How to Upgrade the Manager? on page 5.

- In this section, the term NTBA Appliance refers to the physical as well as the NTBA Virtual Appliances unless mentioned otherwise.

- The following are the minimum required NTBA versions to upgrade to 8.2. These apply to both NTBA appliances and NTBA Virtual Appliances:
  - 7.1.3.6
  - 7.5.3.10
  - 8.0.5.6
  - 8.1.3.6
  - 8.2.7.4

- In release 7.5 and later, in addition to the NTBA Virtual Appliance software (T-VM), the following are also available:
  - NTBA T-100 Virtual Appliance (T-100VM)
  - NTBA T-200 Virtual Appliance (T-200VM)

- You can upgrade your earlier NTBA Virtual Appliance (T-VM) to NTBA T-100VM or T-200VM Virtual Appliance software. However, once you have upgraded, you cannot downgrade. For example, if you have upgraded your NTBA Virtual Appliance software to NTBA T-200VM, you cannot downgrade to NTBA T-100VM or any version of NTBA Virtual Appliance.
• In release 7.5 and later, there are specific images for NTBA T-200 and NTBA T-500 appliances.

  You cannot load software versions across appliances. For example, you cannot load NTBA T-200 image on an NTBA T-500 appliance. The same applies to the NTBA Virtual Appliances as well.

• An 8.x Sensor, for its connections through its management port with NTBA appliances, by default uses NULL cipher (no encryption). Using NULL cipher is required to support the analysis of much larger files. If you want this connection to be encrypted, use the following CLI command on the 8.x Sensor: set amchannelencryption <on><off>. To know if the connection is encrypted, use show amchannelencryption status on the Sensor CLI.

  Enabling encryption can have a performance degradation, which might impact the analysis of large files and high-volume of files.

The upgraded process for an NTBA Appliance is similar to that of a Sensor. So review Sensor software upgrade — Manager versus TFTP server on page 192 and then choose one of the following methods:

- Sensor software and signature set upgrade using Manager 8.2 on page 193:
  - In this section, read Sensor as NTBA Appliance.
  - Ignore the step related to McAfee Custom Attacks.
  - The downloadstatus CLI command is not applicable to NTBA.
  - Failover is not applicable to NTBA.

- Sensor software upgrade using a TFTP or SCP server on page 194:
  - In this section, read Sensor as NTBA Appliance.

---

**Upgrade XC Cluster**

The upgrade for XC Cluster involves upgrade of the Manager, the M-8000XC Sensors, and the XC-240 Load Balancer Device. You can also upgrade just the Manager and continue with the older versions for the M-8000XC Sensors and the XC-240 Load Balancer.

The following are the changes in the XC-240 2.11.x when compared to the earlier versions:

- In XC-240 2.10.X, the lbg set command has a parameter, ha=rebalance ha=loopback. This is no longer available in the 2.11.X.

  Even in the earlier versions, McAfee recommends you to not use ha=rebalance ha=loopback.

- In the XC-240 2.11.x, the output of the pg show command is modified. The parameter Operating mode is changed to Operating Status. Also, the parameter Administrative State is introduced.

- In XC-240 2.11.X, the port show command has changed. The parameters tag and tpid which are present in XC-240 2.10.x are removed in XC-240 2.11.x.

- The file parameter in the config export command is removed in the XC-240 2.11.x.

- The del command is removed in XC-240 2.11.x.
Following are the high-level steps to upgrade a XC Cluster Load Balancer solution:

1. Make sure you have upgraded the Manager to 8.2. See How to Upgrade the Manager? on page 5.

2. Upgrade all the M-8000XC Sensors in a cluster to 8.2. The upgrade process for an XC Cluster Sensor software is similar to that of a Sensor. So review Sensor software upgrade — Manager versus TFTP server on page 192 and then choose one of the methods.

For the minimum required versions for the M-8000XC Sensors to upgrade to 8.2, see Sensor upgrade requirements on page 189.

When you upgrade an M-8000XC Sensor, the Manager pushes the signature set to all the Sensors in the cluster. You can ignore the failed running tasks messages and fault messages displayed in the Manager. These messages are raised because not all the Sensors in the cluster are upgraded to 8.2.

3. Optionally, use the upgrade command to upgrade the XC-240 Load Balancer device to bal_021109_013114. This command is explained in detail in the XC Cluster Administration Guide.

The following are the minimum required versions:

- bal_020902_121611
- bal_021004_060412
- bal_021107_041913

Notes:

- You must always upgrade the Sensors before you upgrade XC-240.
- In case of stand-alone XC-240, there is a network downtime when you upgrade the XC-240. To avoid this downtime, you can use a fail-open switch.
- For high-availability setups, refer to the scenarios described below in this section.
- If you have a configuration higher than n, make sure you upgrade the template Sensor first and then upgrade other Sensors.

Upgrading an N configuration (without Sensor redundancy)

If you have deployed an N configuration, that is without Sensor redundancy, follow this process to upgrade:

![Diagram of XC-240 Load Balancer device and M-8000XC Sensors]
1. Make sure the Managers are upgraded to the latest 8.2 version.
2. Upgrade Sensor 1 (template) to the latest 8.2 version.
3. Upgrade Sensor 2 to the latest 8.2 version.
4. If required, upgrade XC-240 (secondary) to bal_021109_013114.
5. If required, upgrade XC-240 (primary) to bal_021109_013114.

If you have deployed an N+1 configuration, that is with Sensor redundancy, follow this process to upgrade:
1. Make sure the Managers are upgraded to the latest 8.2 version.
2. Upgrade Sensor 1 (template) to the latest 8.2 version.
3. Upgrade the Sensor 2 to the latest 8.2 version.
4. Upgrade the spare Sensor to the latest 8.2 version.
5. If required, upgrade XC-240 (secondary) to bal_021109_013114.
6. If required, upgrade XC-240 (primary) to bal_021109_013114.
Uninstalling the upgrade

Before you begin

- Make sure you downgrade the Sensors before you downgrade the Manager. Similarly, you must downgrade the Managers before you downgrade a Central Manager.
  
  To downgrade Sensor software, see the relevant McAfee KnowledgeBase articles.

- Make sure you have the database backup from the Manager version that you want to downgrade to. For example, if you want to downgrade from 8.2 to 8.1, then you must have the database backup from 8.1 Manager.

If for some reason the upgrade is not suitable, you can uninstall the 8.2 version and reinstall the previous version.

Task

1. Stop the Manager service by following one of these steps:
   - Right-click on the Manager icon at the bottom-right corner of your server and stop the service.
   - Select Windows Control Panel | Administrative Tools | Services. Then right-click on McAfee Network Security Manager and select Stop.

2. Stop the McAfee Network Security Manager Watchdog service using the same method as described in step 1.

3. Uninstall the 8.2 software that you upgraded to.

4. Delete the Network Security Platform install directory (including the MySQL install directory).

5. Reinstall the earlier version from which you upgraded.

6. Restore the corresponding database backup.
   For example, if you had downgraded from 8.2 to 8.1, then restore your 8.1 database backup.
   
   Downgrade all Managers prior to the Central Manager downgrade.
Here are answers to frequently asked questions.

1 I am using Manager version 8.0.x.x. Can I directly upgrade to the latest 8.2?
   Recommend that you upgrade to a supported 8.1 or an earlier 8.2 version before you upgrade to the latest 8.2 version. For details, see Upgrade requirements for the Manager on page 147.

2 Can I upgrade my 8.0 MDR setup directly to 8.2?
   Recommend that you first upgrade your 8.0 MDR setup to a minimum required 8.1 or 8.2 version to upgrade to the latest 8.2 version. To do this:
   a. Click **Switch Over** to make the secondary Manager active.
   b. Upgrade the primary to a minimum as applicable.
   c. Bring up the upgraded primary Manager.
   d. Stop the secondary Manager.
   e. Click **Switch Back** to make the primary Manager active.
   f. Upgrade the secondary Manager to the same 8.x version as the primary.
   g. Bring up the upgraded secondary Manager.

3 In an MDR setup, after upgrading the primary Manager to 8.2, can I switch over to make the primary active or do I have to first stop the secondary?
   Yes. You must stop the secondary. For details, see MDR Manager upgrade on page 182.

4 Do I need to do any specific step after the upgrade to re-establish MDR?
   No. It will work automatically.

5 After upgrading the Secondary Manager, do I need to import the database to secondary or will that happen when I re-establish MDR?
   You must explicitly import the database into the secondary.

6 Do I need to reconfigure MDR to get primary and secondary into MDR again?
   No. The MDR configuration will be retained and will work automatically.

7 Is it safe to assume that the database gets converted from 7.x to 8.2 as part of the 8.2 upgrade?
   Yes.

8 I see the **Switch Over** button in the interface but I have read that I must use the "Switch Back" button to make the primary Manager active. Which is correct?
   The **Switch Over** button in the interface changes to **Switch Back** for the primary to take control from the secondary.
9 If I downgrade the Managers following the instructions in the Network Security Platform 8.2 Installation Guide, I will end up with 7.x Managers and 8.2 Sensors. How do I downgrade the Sensors?

   Downgrading Sensors is a complex process. Contact McAfee Support to first downgrade the Sensors and then downgrade the Manager.

10 Do I really need to upgrade the OS to Windows 2008 or Windows 2012 server for 8.2; can I not continue with my 2003 Server setup?

   No. You must upgrade to one of the supported operating systems to use Network Security Platform 8.2.

11 When do I run the additional offline scripts?

   Additional offline scripts need to be run after completion of upgrade, and only if prompted.
Index

A
about this guide 7
additional scripts 184, 185
anti-virus software 22
authenticated proxy server 97
Authenticated Proxy server 71, 72, 78

B
Browser display settings 17

C
cable specifications 53
Central Manager
  shutting down 47
Central Manager upgrade
  MDR; standalone; system requirements 139
Central Manager; operating system; installation and upgrade 180
Central Manager; upgrade 139
client connections
  closing 47
communication 57
configuration 56, 101
control panel
  shutting down 48
conventions and icons used in this guide 7
custom attacks
  backing up 143, 180
database backup 143, 150, 179
database requirements
  determine 19
  MySQL 18
dedicated interface 26
dedicated server 13
desktop firewall
  installing 20
device
  add 72
device access
  manage 105
device configuration
  update 79, 81
device configuration; troubleshooting 104
Device installation wizard 64
devices
  configure 63
  configure; manage 101
delete 78
diagnostics trace
  upload 104
documentation
  audience for this guide 7
  product-specific, finding 8
typographical conventions and icons 7
downgrade 201

F
fail-closed dongle specification 54
fail-open functionality
  about; fail-closed functionality 83, 97
failover pairs
  manage 95
fiber-optic ports 52
file reputation 150, 152–154, 174
frequently asked questions 203
functional requirements 20

G
Global Threat Intelligence participation 162

H
heterogeneous environments 127
  feature support 137
  large deployments 128
  managing 127
  upgrade paths 129
heterogenous environments
  NTBA devices 137
  upgrade paths; Central Manager 129
  upgrade paths; Manager 133
  XC Cluster 138
Index

I
in-line mode 103
installation
   planning 19
   pre-requisites 19
IP addresses
   allocate 108

J
java runtime engine 18

M
Manager installation; local service account 16
Manager re-design 137
Manager specifications 18
Manager uninstallation; Central Manager uninstallation 113
   add/remove program 113
   using script 115
Manager upgrade
   MDR; standalone; system requirements 147
Manager; Central manager
   downloading executable 24
Manager; Central Manager
   installation 25
   shutting down 46
   start 45
McAfee ServicePortal, accessing 8
MDR Central Manager upgrade 143
MDR Manager upgrade 182

N
network topology 51
new NMS users
   add 106
NMS 105
NMS IP address; new
   add 108
NMS IP addresses
   delete 109
   manage 108
NMS user
   assign 106
   delete 108
   edit 107
NMS users 106
NTBA
   upgrade appliance software 197
NTP server 98, 99

O
offline devices
   export software 87, 89
   software; update 88
   offline devices (continued)
      update 86
   offline download 89
   offline signature set update 85, 86
   OS installation 181
   OS upgrade 180

P
port pin-outs 54–56
pre-installation 13
pre-requisites
   installation 13
preparation for the upgrade
   Central Manager; Manager 141, 149

Q
QoS 151, 158, 175

R
requirements
   Network Security Platform upgrade 120

S
safety warnings 52
secondary Manager IP
   add 62
   remove 62
Sensor
   configure; CLI 67
Sensor
   add 51, 66
   configure 56, 58
   install 51
   unpack 53
Sensor box contents 53
Sensor installation wizard 64
Sensor IP; Manager IP
   change 62
Sensor naming scheme 57
Sensor or NTBA Appliance
   update configuration 102
sensor responsibilities 70
Sensor software upgrade 193
   failover pair 195
   Manager versus TFTP server 192
   TFTP server 194
Sensor software; update 191
Sensor statistics 64
Sensor to Manager
   add 57
Sensor values; change 61
Sensor; NTBA appliance
   shut down 104
Sensors
  install 63
server requirements 14
ServicePortal, finding product documentation 8
signature set
  offline download 87
signature set update 64
signature set upgrade
  Central Manager 146
signature set upgrade; Sensor software upgrade 189
signature sets
  import 65
software update files
  download; offline devices 84
successful configuration
  verifying 61
system requirements
  Central Manager; Manager 140, 148
system requirements; client 16

T
TACACS+ authentication 105
technical support, finding product information 8
third-party applications 14
troubleshooting 42

U
update server
  configuring 111
Update Server
  signature updates; updates 65
upgrade 119, 189
  Central Manager 142
  Manager 149
  Sensors 190
upgrade path
  Central Manager 139, 147
  Manager 139, 147
usage restrictions 53
user interface; MySQL 23

V
VirusScan; SMTP 23
VMware platform 15
Vulnerability Manager 157, 160, 163, 176–178

X
XC Cluster
  upgrade software 198