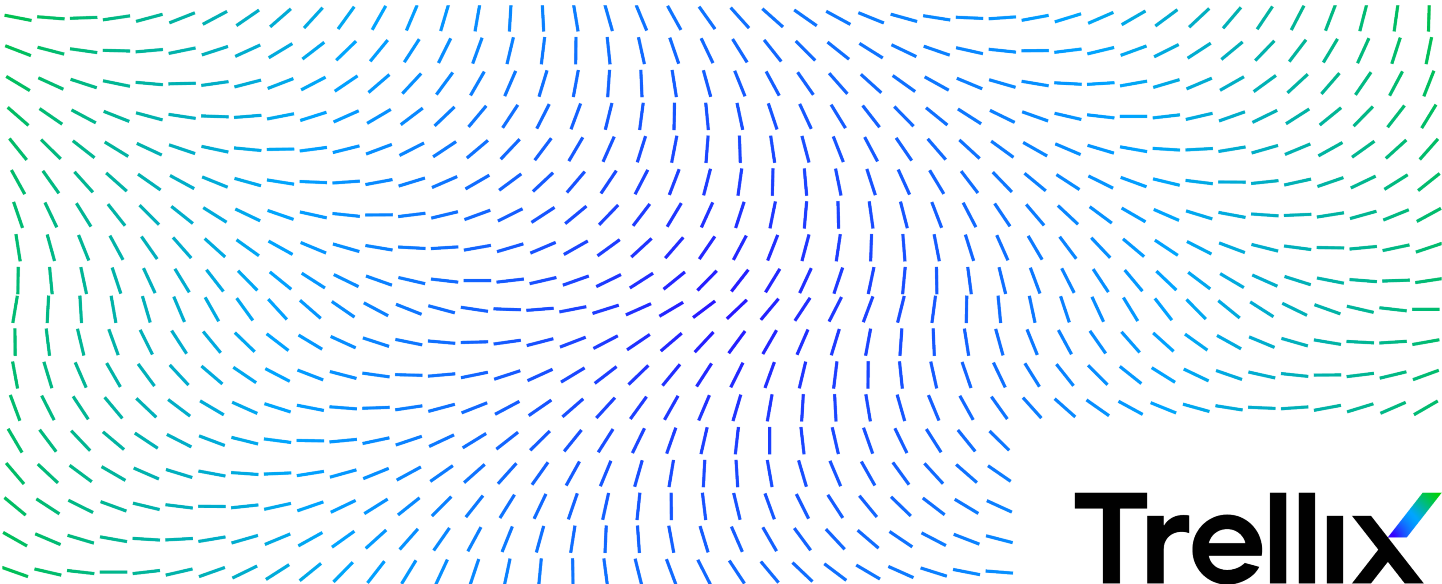


# Trellix Intrusion Prevention System 11.1.x Installation Guide



# Contents

---

<b>Installing Trellix Intrusion Prevention System. . . . .</b>	<b>10</b>
Trellix Intrusion Prevention System overview. . . . .	10
Preparation for the Manager installation. . . . .	10
Prerequisites. . . . .	10
General settings. . . . .	10
Other third-party applications. . . . .	12
Server requirements. . . . .	12
How to host the Manager on virtualization platforms. . . . .	15
Manager installation with local service account privileges. . . . .	16
Client requirements. . . . .	17
Manager client display settings (Windows). . . . .	18
Disk space requirements. . . . .	19
Database requirements. . . . .	19
Recommended Manager specifications. . . . .	20
Determine your database requirements. . . . .	20
Pre-installation recommendations. . . . .	21
How to plan for installation. . . . .	21
Functional requirements. . . . .	21
Install a desktop firewall. . . . .	22
How to use anti-virus software with the Manager. . . . .	23
Trellix Endpoint Security and SMTP notification. . . . .	24
Exclude On-Access Scan of Manager components. . . . .	24
Exclude On-Demand Scan of Manager components. . . . .	25
Turn off Real-time protection in Windows Server 2019. . . . .	25

User interface responsiveness. ....	30
Download the Manager/Central Manager executable. ....	30
Install the Manager/Central Manager. ....	31
Install the Manager. ....	32
Install the Manager on Windows server. ....	32
Installing the Central Manager. ....	44
Launch virtual instance of the Manager on MLOS. ....	45
Create a Manager instance using OVA file. ....	45
Create a Manager instance using qcow2 file. ....	50
Dual NIC support in Linux based Manager. ....	55
Configure the Manager on MLOS. ....	56
Log files related to Manager installation and upgrade. ....	59
Product Registration. ....	60
Obtain the Trellix IPS Registration Key. ....	61
Register the IPS Manager with Trellix. ....	61
Starting the Manager/Central Manager. ....	63
CA-signed certificate for the Web Server Authentication. ....	65
Considerations for CA-signed certificate for the Web Server Authentication. ....	65
Import the CA-signed certificate for Web Server Authentication. ....	65
Export the CA-signed certificate for Web Server Authentication. ....	67
Delete the CA-signed certificate for Web Server Authentication. ....	68
Authentication of access to the Manager using CAC/PIV. ....	68
Obtain the CA certificates. ....	69
Import the CA certificates. ....	70
Set up CAC users in the Manager. ....	72
Enable the CAC authentication. ....	73
Log on to the Manager using the CAC/PIV authentication. ....	76
Troubleshooting tips. ....	76
Shut down the Manager/Central Manager services. ....	76
Shut down the Central Manager. ....	77

Close all the client connections. ....	77
Shut down using the Trellix IPS Manager system tray icon in the Windows based Manager. ....	77
Shut down using the Control Panel in the Windows based Manager. ....	78
Shutdown using the Manager shell in the Linux based Manager. ....	80
Adding a Sensor. ....	80
Before you install Sensors. ....	81
Network topology considerations. ....	81
Safety measures. ....	81
Fiber-optic ports. ....	83
Usage restrictions. ....	83
Unpack the Sensor. ....	83
Contents of the Sensor box. ....	84
Cable specifications. ....	84
Console port pin-outs. ....	84
Auxiliary port pin-outs. ....	85
Management port pin-outs. ....	86
Response port pin-outs. ....	86
How to monitor port pin-outs. ....	87
Gigabit Ethernet (GE) ports. ....	87
Configuration of a Sensor. ....	87
Configuration overview. ....	88
Establishment of a Sensor naming scheme. ....	88
Communication between the Sensor and the Manager. ....	89
Add a Sensor to the Manager. ....	89
Configure the Sensor. ....	91
Verification of successful configuration. ....	93
How to change Sensor values. ....	94
Change the Sensor IP or the Manager IP. ....	94
How to add a secondary Manager IP. ....	95
Remove a secondary Manager IP. ....	96

Configuration of devices using the Manager. ....	96
Add and configure Sensors. ....	96
Add a Sensor to the Manager. ....	96
Configure the Sensor using CLI. ....	97
Managing licenses for NS9500, NS7500, and NS3500 Sensors. ....	99
Add license to the Manager. ....	103
Assign a license to a Sensor. ....	104
Unassign a license from a Sensor. ....	106
Upgrade an existing capacity license. ....	106
Remove a license from the Manager. ....	111
Possible actions from the device list nodes. ....	111
Options available in the Devices page. ....	112
Edit device settings. ....	112
Delete a device configuration. ....	113
Deploy pending changes to a device. ....	115
Update the latest software images on all devices. ....	118
Download software update files for offline devices. ....	122
Configure a new device for indirect mode signature set update. ....	123
Configure an existing device for indirect mode signature set update. ....	124
Update configuration for offline devices. ....	125
Export device configuration. ....	126
Perform an offline download of the signature set. ....	127
Update software for offline devices. ....	127
Export device configuration. ....	128
Import software for offline devices. ....	129
Malware engine updates. ....	129
Gateway Anti-Malware update. ....	130
Set up automatic updates for Gateway Anti-Malware Engine for a domain. ....	130
Set up automatic updates for Gateway Anti-Malware Engine for a device. ....	131
Update Gateway Anti-Malware Engine manually. ....	133

Manage HA pairs. ....	141
Specify proxy server for internet connectivity. ....	145
Configure NTP server for a domain. ....	146
Configure NTP server for a device. ....	148
Managing configuration for each device. ....	151
Configuration and management of devices. ....	151
Update configuration of a Sensor. ....	152
Update software for a Sensor. ....	154
Shut down a Sensor. ....	155
Troubleshooting your device configuration. ....	156
Upload diagnostics trace. ....	156
Management of device access. ....	157
Configure TACACS+ authentication. ....	157
Configuration of NMS objects. ....	158
Management of NMS users. ....	158
Assign an NMS user. ....	159
Add a new NMS user. ....	159
Edit an NMS user. ....	161
Delete an NMS user. ....	161
Management of NMS IP addresses. ....	162
Allocate an IP addresses. ....	162
Add a new NMS IP address. ....	162
Delete NMS IP addresses. ....	163
Configuration of the Update Server. ....	164
Uninstallation of the Manager/Central Manager. ....	164
Uninstall using the Add/Remove program. ....	164
Uninstall using the script. ....	167
<b>Upgrading Trellix Intrusion Prevention System. ....</b>	<b>168</b>
Overview. ....	168
Important requirements and considerations. ....	169

Management of a heterogeneous environment. . . . .	169
What are heterogeneous environments?. . . . .	169
When would you need a heterogeneous environment?. . . . .	171
Upgrade scenarios for heterogeneous environments. . . . .	171
Central Manager upgrade scenarios. . . . .	171
Scenario 1 – Homogeneous, standalone setup. . . . .	172
Scenario 2 – Homogeneous, MDR setup. . . . .	173
Scenario 3 - Heterogeneous, standalone setup. . . . .	174
Scenario 4 - Heterogeneous, MDR setup. . . . .	175
Manager upgrade scenarios. . . . .	176
Scenario 5 - Homogeneous, standalone setup. . . . .	176
Scenario 6 - Homogeneous, MDR setup. . . . .	177
Scenario 7 - Heterogeneous, standalone setup. . . . .	178
Scenario 8 – Heterogeneous MDR. . . . .	179
Heterogeneous support for NTBA devices. . . . .	180
How to upgrade the Central Manager?. . . . .	181
Upgrade requirements for the Central Manager. . . . .	181
Upgrade path for the Central Manager. . . . .	181
Considerations for Linux based Central Manager/Manager. . . . .	183
Central Manager and Manager system requirements. . . . .	183
Preparation for the upgrade. . . . .	188
Backing up Trellix IPS data. . . . .	188
Perform a database backup. . . . .	188
Back up Trellix IPS custom attacks. . . . .	189
Review the upgrade considerations. . . . .	189
Notes for upgrading the Central Manager from 10.1 to 11.1. . . . .	189
Central Manager and operating system upgrade. . . . .	190
Standalone Central Manager upgrade. . . . .	190
Upgrade the signature set for the Central Manager. . . . .	191
MDR Central Manager upgrade. . . . .	192

How to Upgrade the Manager? .....	193
Upgrade requirements for the Manager. ....	193
Upgrade path for the Manager. ....	193
Considerations for Linux based Central Manager/Manager. ....	194
Central Manager and Manager system requirements. ....	194
Preparation for the upgrade. ....	199
Manager upgrade downtime window. ....	199
Database backup (before and after upgrade). ....	199
Notes for upgrading the Manager from 10.1 or 11.1 to 11.1.7.71. ....	200
Notes for upgrading the Manager from 10.1 or 11.1 to 11.1.7.56. ....	205
Notes for upgrading the Manager from 10.1 or 11.1 to 11.1.7.41. ....	207
Notes for upgrading the Manager from 10.1 or 11.1 to 11.1.7.26. ....	215
Notes for upgrading the Manager from 10.1 to 11.1. ....	219
Backing up Trellix IPS data. ....	223
Perform a database backup. ....	223
Back up Trellix IPS custom attacks. ....	223
Operating system upgrade for Windows based Manager. ....	224
Manager and operating system upgrade. ....	224
Approach 1: Upgrade the operating system and the Manager. ....	224
Approach 2: Using new hardware. ....	225
Standalone Manager upgrade on Windows operating system. ....	226
Standalone Manager upgrade on Linux operating system. ....	229
Root partition extension in Linux-based Manager. ....	234
MDR Manager upgrade. ....	237
How to perform signature set and Sensor software upgrade. ....	237
Difference between an update and an upgrade. ....	237
Signature set upgrade. ....	238
Sensor software upgrade requirements. ....	238
Review the upgrade considerations for Sensors. ....	241
Notes for upgrading the Sensor from 10.1 or 11.1 to 11.1.5.72. ....	241



Note about upgrading the Sensor from 10.1 or 11.1 to 11.1.5.56 or 11.1.5.57. ....	246
Note about upgrading the Sensor from 10.1 or 11.1 to 11.1.5.44. ....	248
Note about upgrading the Sensor from 10.1 or 11.1 to 11.1.5.22. ....	251
Note about upgrading the Sensor from 10.1 to 11.1. ....	254
Updating Sensor software image. ....	255
Sensor software upgrade — Manager versus TFTP server. ....	257
Sensor software and signature set upgrade using Manager 11.1. ....	257
Sensor software upgrade using a TFTP or SCP server. ....	260
Update Sensor software in a HA pair. ....	261
Uninstalling the upgrade. ....	262
Windows based Manager: Frequently asked questions. ....	263

# Installing Trellix Intrusion Prevention System

This section of the guide provides information on how to install Trellix Intrusion Prevention System.

:

## Trellix Intrusion Prevention System overview

Trellix Intrusion Prevention System 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. Trellix Intrusion Prevention System 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 Trellix Intrusion Prevention System Manager (Manager) hardware and software requirements and pre-installation tasks that you should perform prior to installing the software.

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

:

### Prerequisites

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

#### Caution

We strongly recommend that you also review the Trellix Intrusion Prevention System Release Notes.

:

### General settings

#### Windows based Manager

- Trellix 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 Trellix IPS Manager software and an embedded database for Windows Manager during Manager installation.
- It is essential that you synchronize the time on the IPS 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 Trellix Intrusion Prevention System Sensors (Sensors) and the Trellix 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.)



### Tip

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



### Note

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.

## Linux based Manager

- 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 Trellix Intrusion Prevention System Sensors (Sensors) and the Trellix 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.)



### Tip

For more information about setting up a time server on Linux based Manager, see the following Man page article: <http://man7.org/linux/man-pages/man1/timedatectl.1.html>.



### Note

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 Attack Log 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 Trellix IPS Sensors. For more information on downloading and using Wireshark, go to [www.wireshark.org](http://www.wireshark.org).

### Note

Installation of third-party applications is not supported in the Linux based Manager.

:




## Server requirements

The following table lists the 11.1 Windows based Manager/Central Manager application requirements:

### Note


Windows Server 2012 Standard/Windows Server 2012 R2 Standard is not supported for the Manager.

	Minimum required	Recommended
Operating system	Any of the following: <ul style="list-style-type: none"> <li>Windows Server 2016 Standard Edition English operating system</li> <li>Windows Server 2016 Standard Edition Japanese operating system</li> <li>Windows Server 2016 Datacenter Edition English operating system</li> <li>Windows Server 2016 Datacenter Edition Japanese operating system</li> </ul>	Windows Server 2022 Datacenter Edition operating system

	Minimum required	Recommended
	<ul style="list-style-type: none"> <li>Windows Server 2019 Standard Edition English operating system</li> <li>Windows Server 2019 Standard Edition Japanese operating system</li> <li>Windows Server 2019 Datacenter Edition English operating system</li> <li>Windows Server 2019 Datacenter Edition Japanese operating system</li> <li>Windows Server 2022 Standard Edition English operating system</li> <li>Windows Server 2022 Standard Edition Japanese operating system</li> <li>Windows Server 2022 Datacenter Edition English operating system</li> <li>Windows Server 2022 Datacenter Edition Japanese operating system</li> </ul> <div style="background-color: #e1f5fe; padding: 5px; margin-top: 10px;">  <b>Note:</b> Only x64 architecture is supported.                 </div>	
Memory	16 GB <div style="background-color: #e1f5fe; padding: 5px; margin-top: 10px;">  <b>Note:</b> Supports up to 10 million alerts in Solr                 </div>	>=32 GB <div style="background-color: #e1f5fe; padding: 5px; margin-top: 10px;">  <b>Note:</b> Supports up to 20 million alerts in Solr                 </div>
CPU	Server model processor, such as Intel Xeon	Same

	Minimum required	Recommended
Disk space	300 GB	500 GB or more
Network	1 Gbps card	1 Gbps card
Virtual CPUs (Applicable only on a VMware platform)	4	4 or more

The following table lists the 11.1 Linux based Manager/Central Manager application specifications for an OVA file:

Component	Specifications
MLOS	3.9.1
Logical CPU cores	8
Memory	32 GB
Disk space	500 GB
NIC	1
	 <b>Note:</b> You can consider 2 for a dual NIC configuration.

The following table lists the 11.1 Linux based Manager/Central Manager application specifications for a qcow2 file:

Component	Specifications
MLOS	3.9.1
Logical CPU cores	8
Memory	20 GB


Component	Specifications
Disk space	500 GB
NIC	1

:

## How to host the Manager on virtualization platforms


### VMWare ESXi

VMware ESXi server requirements for Windows Operating System

Component	Supported
Virtualization software	<ul style="list-style-type: none"> <li>ESXi 7.0 Update 3</li> <li>ESXi 8.0</li> </ul> <div style="background-color: #e0f2f7; padding: 5px; margin-top: 10px;">  <b>Note:</b> Hyperthreading should be available.                 </div>

The following are the system requirements for hosting 11.1 Linux based Manager/Central Manager application on a VMware platform:

VMware ESXi server requirements for MLOS

Component	Supported
Virtualization software	<ul style="list-style-type: none"> <li>ESXi 7.0 Update 3</li> <li>ESXi 8.0</li> </ul> <div style="background-color: #e0f2f7; padding: 5px; margin-top: 10px;">  <b>Note:</b> Hyperthreading should be available.                 </div>

### Kernel-based Virtual Machine (KVM)

The following are the system requirements for hosting 11.1 Linux based Manager/Central Manager application on KVM:

KVM server requirements for MLOS

Component	Supported
Virtualization software	KVM 2.12.0

:

### Manager installation with local service account privileges

The Manager installs the following services as a Local Service:

- Trellix IPS Manager
- Trellix IPS Manager Database

#### Note

Trellix IPS Manager Watchdog runs as a Local System to facilitate restart of the Manager in case of abrupt shutdown.

#### Note

Manager installation with local service account privileges is not supported in the Linux based Manager.

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 the 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 MariaDB database configured for using a directory for temporary files other than the one provided during installation, those directories should be given full permissions for a Local Service.

:

## Client requirements

The following table lists the 11.1 Manager/Central Manager client requirements when using Windows 10:

	Minimum	Recommended
Operating system	Windows 10, English or Japanese   <b>Note:</b> The display language of the Manager client must be same as that of the Manager server operating system.	Windows 10, version 1903 English or Japanese
Memory	8 GB	16 GB
CPU	1.5 GHz processor	2.4 GHz or faster
Monitor	32-bit color, 1440 x 900 display setting	1920 x 1080 (or above)
Browser	<ul style="list-style-type: none"> <li>• Microsoft Edge</li> <li>• Mozilla Firefox</li> <li>• Google Chrome</li> </ul>  <b>Note:</b> To avoid the certificate mismatch error and security warning, add the Manager web certificate to the trusted certificate list.	<ul style="list-style-type: none"> <li>• Microsoft Edge 111.0 or later</li> <li>• Mozilla Firefox 111.0 or later</li> <li>• Google Chrome 111.0 or later</li> </ul>

For the Manager/Central Manager client, in addition to Windows 10, you can also use the operating systems mentioned for the Manager server.

The following table lists the 11.1 Manager/Central Manager client requirements when using Windows 10:

Mac operating system	Browser
Ventura	Safari 16 or later

:

### 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 Desktop and select Screen Resolution and go to Advanced Settings → Monitor, and configure Colors to True Color (32bit).
- Trellix recommends setting your monitor's screen area to 1440 x 900 pixels. Right-click on the Desktop 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.

### Internet Explorer settings when accessing the Manager from the server

Trellix 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.

#### Note

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.

:

### Disk space requirements

The amount of disk space required for the Manager/ Central Manager depends on factors unique to the deployment scenario.

The considerations for the Manager/Central Manager virtual machine disk space are as follows:

- **Trellix IPS Manager** — The disk space required for the Manager mainly determines the size of the Manager database (MariaDB). This decides the number of alerts and packets logs that can be stored. The recommended disk space for the Manager is 300 GB, but it varies based on the deployment scenarios. For example, if you want store alerts and packet logs for 30 days, the recommended disk space is 500 GB.
- **Trellix IPS Central Manager** — The disk space required for the Central Manager mainly determines the size of the Solr database. This decides the number of alerts and packets logs from the Managers that can be displayed in the Central Manager. The MariaDB in the Central Manager occupies a smaller amount of disk space and stores the configuration information of the Central Manager. The overall disk space recommended for the Central Manager is 500 GB.

As a best practice, Trellix recommends archiving and deleting old alert data regularly and trying to keep your active database size to about 60% of the disk space.

:

### Database requirements

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

The Manager installation set includes a database for installation (that is embedded on the target Manager server). You must use the supported operating system listed under *Server requirements*, and the bundles of Manager supplied version for MariaDB and J-connector versions. The MariaDB **must be a dedicated one that is installed** on the Manager.

#### Note

For more information on the latest versions of MariaDB and J-connector, refer to *Trellix Intrusion Prevention System Manager-NS-series Release Notes*.

### Note

If you have MariaDB previously installed on the Manager server, uninstall the previous version and then install the Trellix IPS version.

:

### Recommended Manager specifications

The Manager software runs on a dedicated Windows server.

The larger your deployment, the more high-end your Manager server should be. Many Trellix IPS issues result from an under-powered Manager Server. For example, to manage 40 or more IPS 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 Trellix IPS solution exceed the minimum-required specifications mentioned in *Client requirements*.

### Tip

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 that are 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, Trellix recommends archiving and deleting old alert data regularly and trying to keep your active database size to about 60% of the disk space.

### Note

For more information, see *Capacity Planning* in *Trellix Intrusion Prevention System Product Guide*.

:

### Pre-installation recommendations

These Trellix Intrusion Prevention System pre-installation recommendations are a compilation of the information gathered from individual interviews with some of the most seasoned Trellix IPS System Engineers at Trellix.

:

### How to plan for installation

Before installation, ensure that you complete the following tasks:

- The Windows server, on which the Manager software will be installed, should be configured and ready to be placed online (Not required for Linux based Manager).
- You must have administrator privileges for the Windows based Manager server (Not required for Linux based Manager).
- This Windows 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 (Not required for Linux based Manager).
- 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, Trellix strongly recommends assigning a static IP 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 Trellix IPS Sensors, the use of sub-interfaces or interface groups, and if and how the Manager will be connected to the production network.
- Obtain the required Trellix IPS Registration key, license file, and grant number.
- Accumulate the required number of wires and (supported) SFP, SFP+, QSFP+, or QSFP28 transceivers. Ensure these are approved hardware from Trellix or a supported vendor.
- 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.

:

### Functional requirements

Following are the functional requirements to be taken care of:

- (Applicable to Windows based Manager only) Install Wireshark (formerly known as Ethereal <https://www.wireshark.org>) on the client PCs. Wireshark is a network protocol analyzer used to analyze packet logs created by Sensors on Unix and Windows servers.
- (Applicable to Windows based Manager only) 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 Trellix 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.)
- 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](#).
- (Applicable to Windows based Manager only) If a fresh installation of the Manager is needed on a machine where a Manager is already installed, ensure that the existing Manager is uninstalled and the respective directories are removed prior to the fresh installation.

### Note

Reboot the machine after uninstallation for the removal of directories.

:

## Install a desktop firewall

A desktop firewall on the Manager server is recommended. Certain ports are used by the components of Trellix IPS. Some of these are required for Manager -- Sensor and Manager client-server communication. All remaining unnecessary ports should be closed.

Trellix strongly recommends that you configure a packet-filtering firewall to block connections to ports 8551, 3306, and 8005 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, 3306, and 8005, the firewall should automatically block any packets sent. If you need assistance in blocking these, contact Trellix Technical Support.

### Note

Trellix strongly recommends you not to change the firewall settings in the Linux based Manager.

### Note

Use a scanning tool to ensure that there are 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, refer to the section *Set the desktop firewall* in *Trellix Intrusion Prevention System Manager Product Guide* and open the ports mentioned in the section.

### Note

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.

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.

### Note

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 Trellix Endpoint Security 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.

### Note

During installation or upgrade of the Manager server, you must exclude the `<Manager_Install_Dir>` from the Trellix Endpoint Security or any other anti-virus software scan.

Exclude the following Manager folders from anti-virus scan:

- `<Manager_Install_Dir>\MariaDB` and its sub-folders. If these folders are not excluded, Trellix IPS packet captures may result in the deletion of essential MariaDB files.

- <Manager\_Install\_Dir>\App\temp\tftpin\malware\ and its sub-folders.
- <Manager\_Install\_Dir>\Solr\server\solr>alerts\ and its sub-folders.
- <Manager\_Install\_Dir>\Solr\server\solr\appAlerts\ and its sub-folders.

### Note

Excluding Manager installation directories from anti-virus scan is not required for Linux based Manager.

:

### Trellix Endpoint Security and SMTP notification

Trellix Endpoint Security 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.

Trellix Endpoint Security 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 Trellix Endpoint Security, you must 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, append **java.exe** to the exclusion list of Trellix Endpoint Security On-Access Scan and On-Demand Scan.

:

### Exclude On-Access Scan of Manager components

In some scenarios, Trellix Endpoint Security prevents you from installing/upgrading the Manager application or taking a backup of the Manager database. To avoid such cases, you need to exclude the IPS Manager folder from On-Access Scan. Complete the steps below to exclude the folder from On-Access Scan.

1. Open Trellix Endpoint Security from the Start Menu of the Manager server.
2. Click  → Settings.
3. Click Threat Prevention → Show Advanced → ON-ACCESS SCAN.
4. In the Process Settings section, select Standard tab under process type.
5. Click Add in the Exclusions section.
6. In the Add Exclusions window, click Browse.
7. Select the IPS Manager folder.



### Note


In some cases, the Manager takes advantage of the JavaMail API to send SMTP notifications. If you enable SMTP notification and also run Trellix Endpoint Security, you must add java.exe to the list of excluded processes. If you do not explicitly create the exclusion within Trellix Endpoint Security, 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.

8. In the Add Exclusions window, click Also exclude subfolders. Click OK.
9. For the High Risk and Low Risk process type, repeat steps 5 to 8.
10. Click Apply.

:

### Exclude On-Demand Scan of Manager components

In some scenarios, Trellix Endpoint Security prevents you from installing/upgrading the Manager application or taking a backup of the Manager database. To avoid such cases you need to exclude the IPS Manager folder from On-Demand Scan. Complete the steps below to exclude the folder from On-Demand Scan.

1. Open Trellix Endpoint Security from the Start Menu of the Manager server.
2. Click  → Settings.
3. Click Threat Prevention → Show Advanced → ON-DEMAND SCAN.
4. In the ON-DEMAND SCAN section, select Full Scan tab.
5. Click Add in the Exclusions section.
6. In the Add Exclusions window, click Browse.
7. Select the IPS Manager folder.

### Note

In some cases, the Manager takes advantage of the JavaMail API to send SMTP notifications. If you enable SMTP notification and also run Trellix Endpoint Security, you must add java.exe to the list of excluded processes. If you do not explicitly create the exclusion within Trellix Endpoint Security, 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.

8. In the Add Exclusions window, select Also exclude subfolders. Click OK.
9. For the Quick Scan and Right-Click Scan, repeat steps 5 to 8.
10. Click Apply.

:

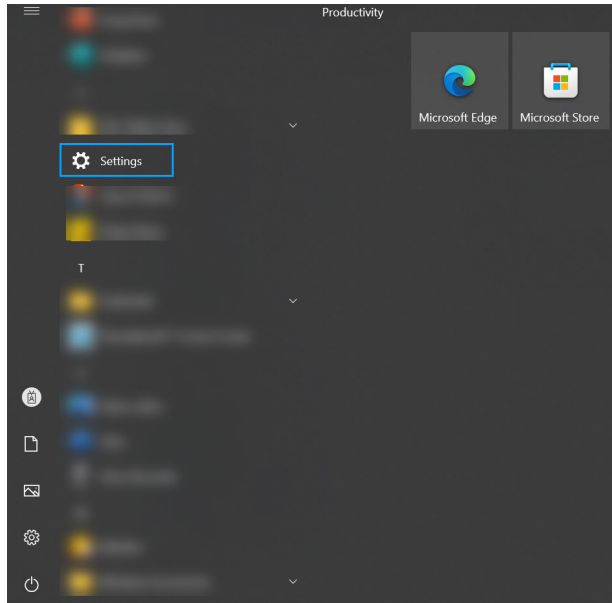
### Turn off Real-time protection in Windows Server 2019

The Real-time protection in Windows server 2019 flags the Manager Apache Solr database as a threat and removes the file. If you have installed the Manager in Windows server 2019, you will have to turn off Real-time protection.

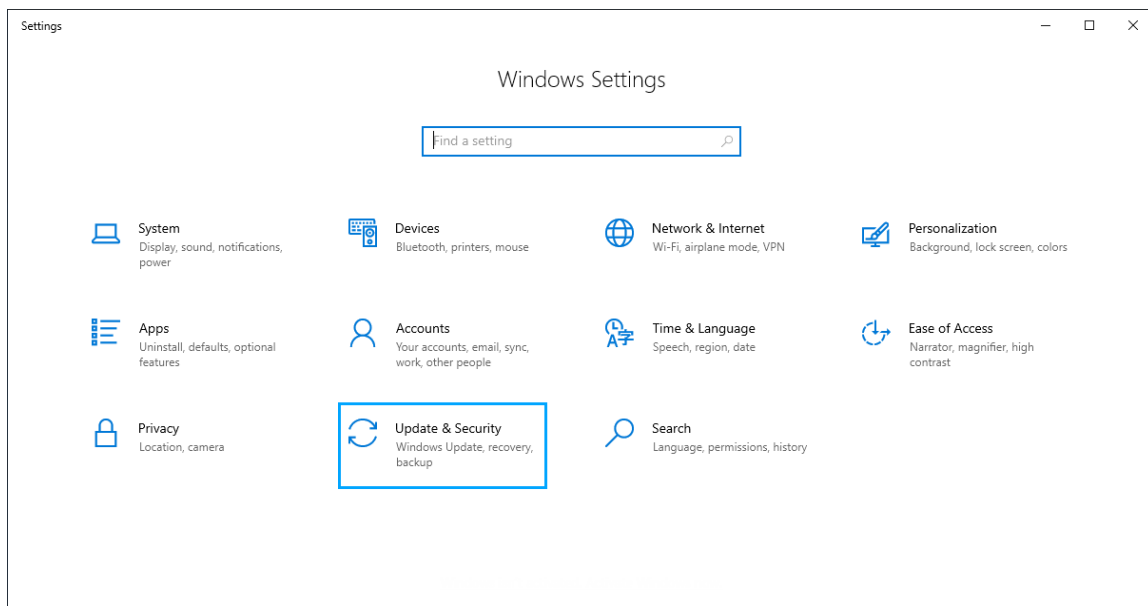
You can turn off Real-time protection either from the Windows Settings or from Windows PowerShell.

### Steps:

1. Follow the steps below to turn-off Real-time protection from Windows Settings:
  - a. Open Settings from the Start Menu of the Manager server.



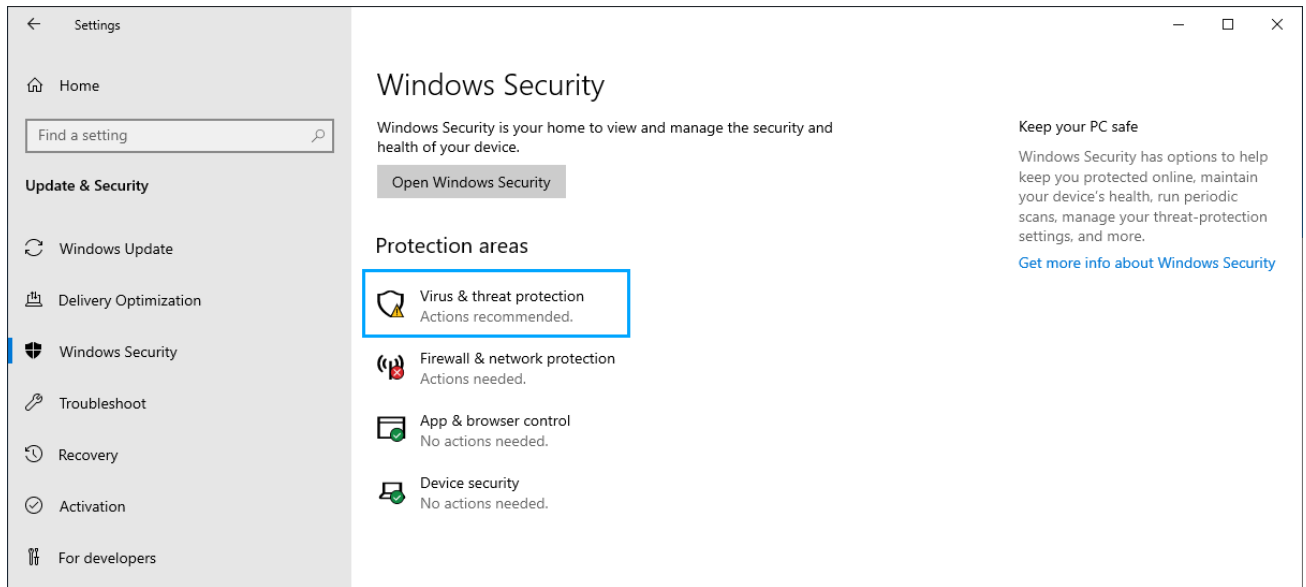
- b. Open the Update & Security settings.



c. Select Windows Security.

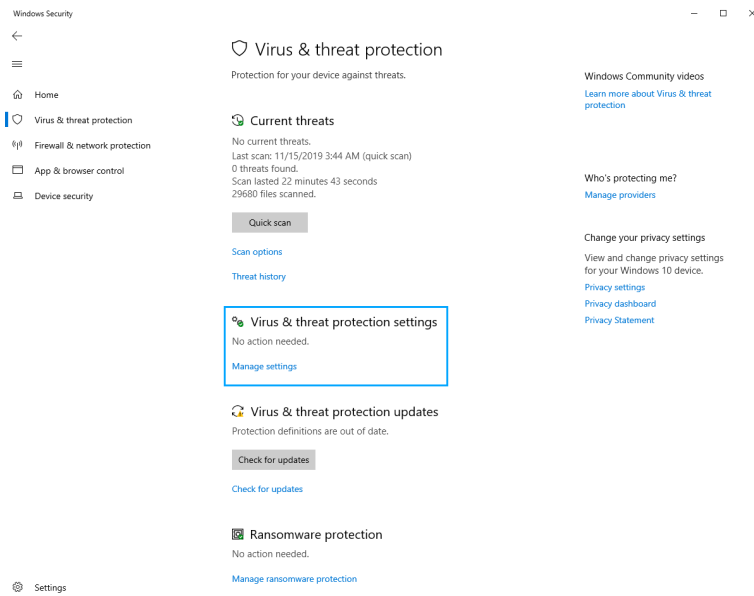


d. Click Virus & threat protection from Protection areas.

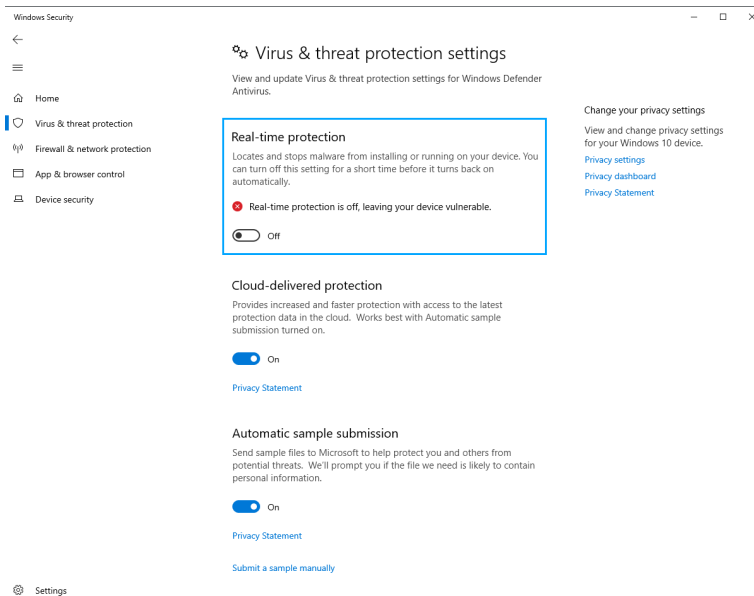


e. Click Manage settings in Virus & threat protection settings.

# 1 | Installing Trellix Intrusion Prevention System

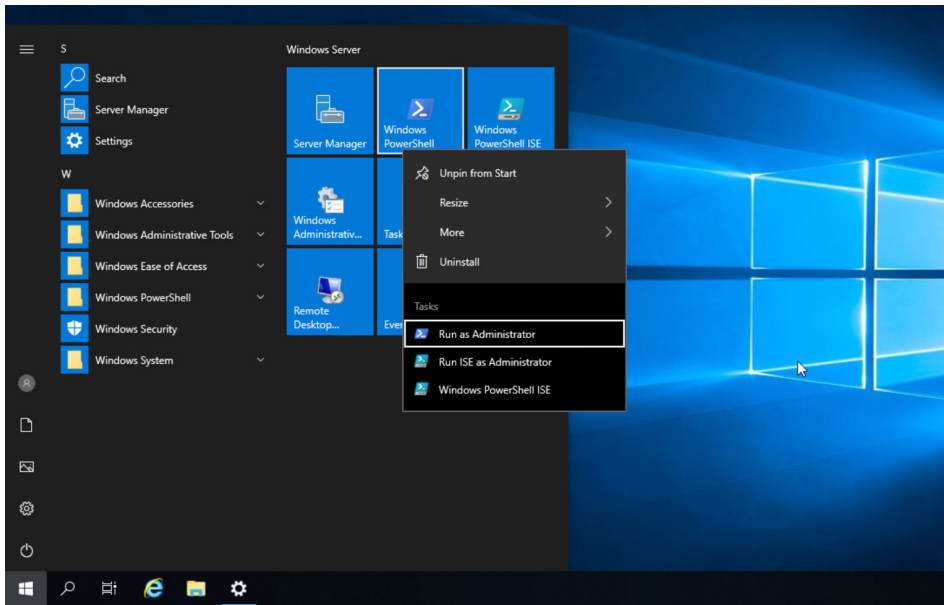


## f. Turn Off Real-time protection.



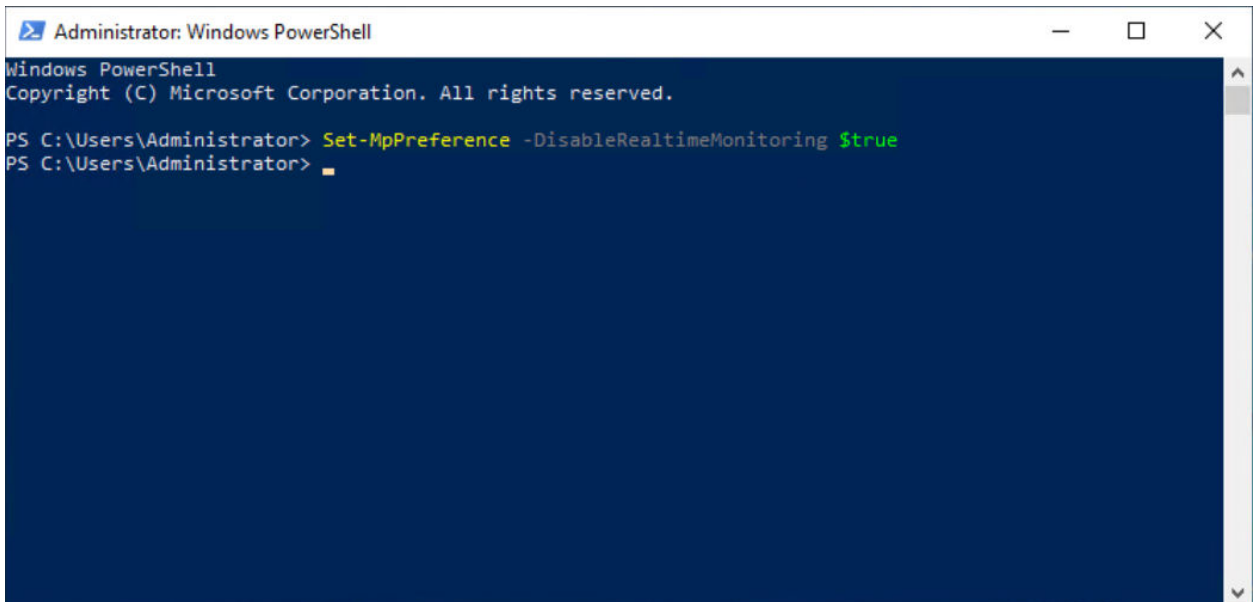
## 2. Follow the steps below to turn-off Real-time protection using Windows PowerShell:

- a. From the Start Menu of the Manager server, run Windows PowerShell as an Administrator.



Windows PowerShell opens with administrative privileges.

- b. Type any one of the following commands and press **Enter** to turn-off Real-time protection on the server:**Set-MpPreference -DisableRealtimeMonitoring \$true**Or**Set-MpPreference -DisableRealtimeMonitoring 1**



:

### User interface responsiveness

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

In this section, we suggest some easy but essential steps to ensure that Trellix IPS 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 for the user interface to parse through those records for display in the Attack Log. The default Trellix IPS 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.

#### Caution

It is imperative that you tune the 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 MariaDB directory. The more often you run your defragmenter, the quicker the process will be. Consider defragmenting the disks at least once a month.

#### Caution

Do NOT attempt to defragment the MariaDB 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 *Trellix Intrusion Prevention System Product Guide*.

- Limit the number of alerts to view when opening the Attack Log. This will reduce the total quantity of records the user interface must parse and, therefore, 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 [Trellix Download Server](#).

### Steps:

1. Keep the following information handy before you begin the installation process. You must have received the following from Trellix via email.
  - Grant Number and Registered Email Address – If you have not received your credentials, contact Trellix [Technical Support](#).
2. Close all open applications.
3. Go to the [Trellix Download Server \(https://www.trellix.com/en-us/downloads/my-products.html\)](https://www.trellix.com/en-us/downloads/my-products.html) and click Download under the Product Downloads section.
4. Log on using the **Grant Number** and **Email Address**.  
The Find Products page opens.
5. Select Network Security under Filters in the right pane.
6. Select Intrusion Prevention System Manager.
7. Select the Type as Installation under Filters in the right pane.
8. Click on the required <IPSM major version number> to download the Manager software.

:

## Install the Manager/Central Manager

### Prerequisites:

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.

### Note

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 or MLOS, including the installation of MariaDB.

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

### Steps:

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, register the Manager with Trellix. See [Product Registration](#).

:

### Install the Manager

The steps presented are for installation of the Manager/ Central Manager software. Read each step carefully before proceeding to the next step.

:

### Install the Manager on Windows server

The steps presented are for installation of the Manager/ Central Manager software on Windows server. 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.

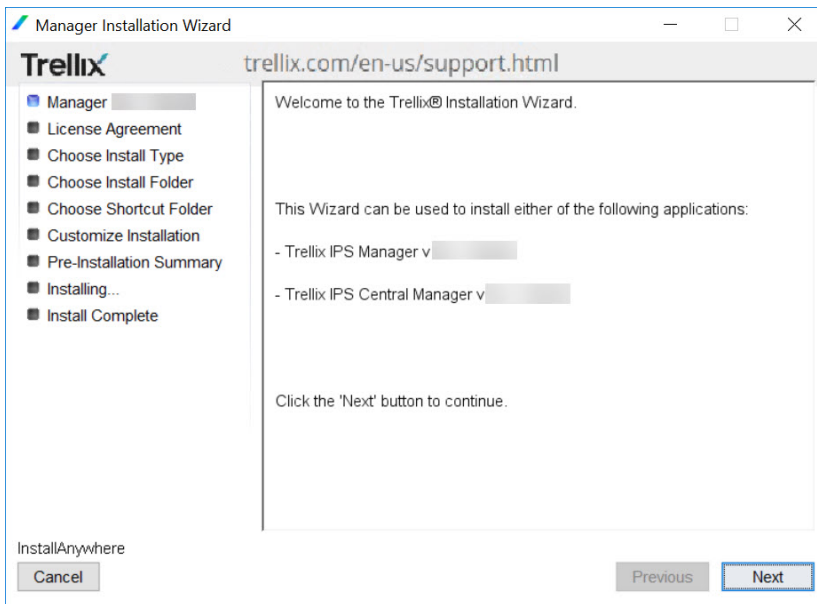
#### Notes:

- 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, Trellix Intrusion Prevention System 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 Trellix Intrusion Prevention System Manager, the default location is <System\_Drive>\Program Files\Trellix\IPS Manager\App. For Trellix Intrusion Prevention System Central Manager, it is <System\_Drive>\Program Files\Trellix\IPS Central Manager\App. Similarly, the Wizard creates default folders for the database as well. For the sake of explanation, this section mentions only the folder paths for Trellix IPS Manager unless it is necessary to mention the path for Trellix IPS 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 2019 Standard or Datacenter Edition, Japanese Operating System (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 Trellix Global Threat Intelligence to send your alert, general setup, and feature usage data to Trellix for optimized protection. If you do not wish to send these data, you should disable the integration with Trellix Global Threat Intelligence. However, note that to be able to query Trellix 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 Trellix. For details, see *Trellix Intrusion Prevention System 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:
  - Uninstall the Manager.
  - Go to the installation directory.
  - Delete all the previous Manager default folders.
  - Once the folders are removed, restart the system and then continue with the Manager installation.

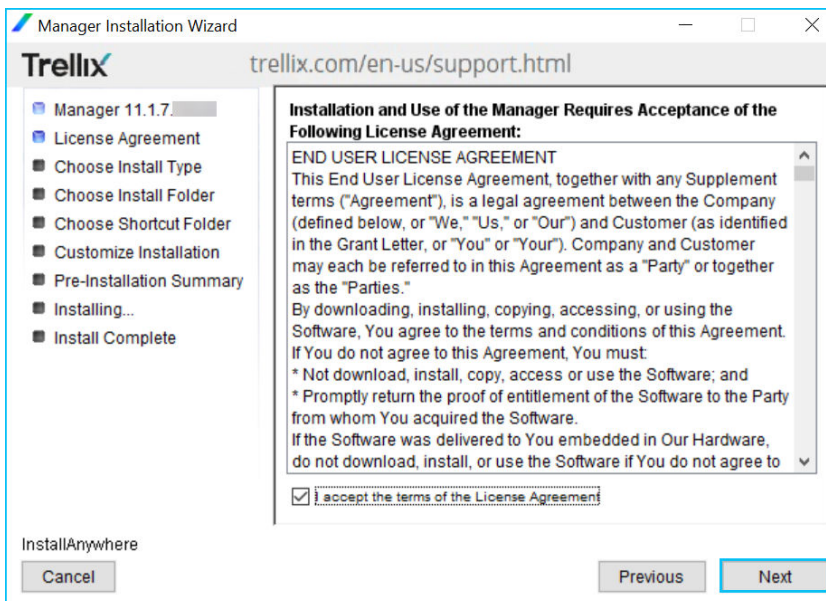
#### Steps:



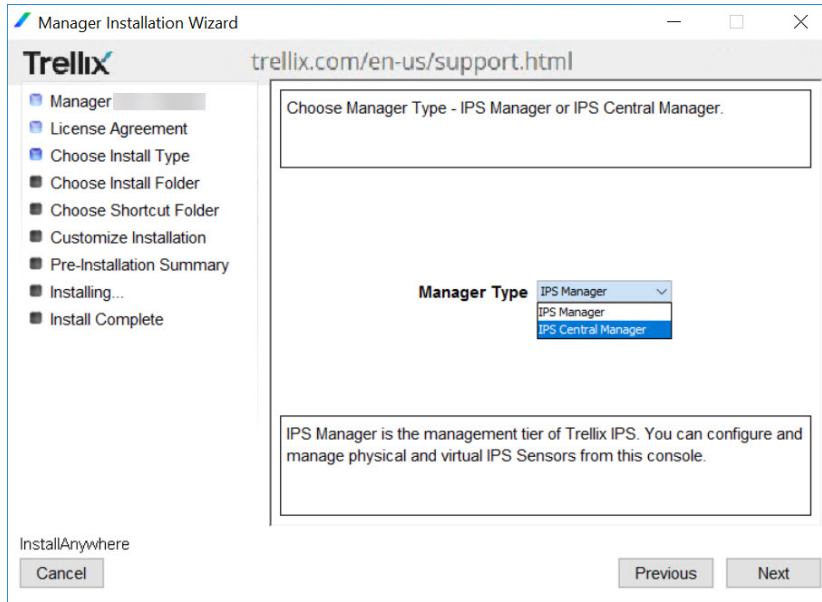
1. Log on to your Windows server as Administrator and close all open programs.
2. Run the Manager executable file that you downloaded from the Trellix Download Server. The Installation Wizard starts with an introduction screen. See also the [Download the Manager/Central Manager executable](#).



3. Confirm your acknowledgment of the License Agreement by selecting I accept the terms of the License Agreement.



4. From the Manager Type drop-down list, select IPS Manager or IPS Central Manager. For an upgrade, IPS Manager or IPS Central Manager is displayed accordingly, which you cannot change.



### Note

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

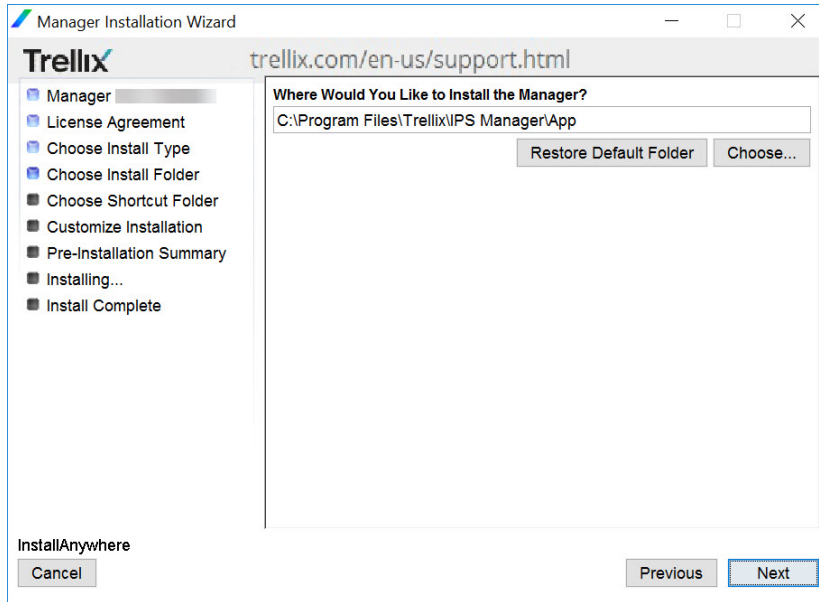
5. Choose a folder where you want to install the Manager software. For a first-time installation, the default location is `<System_Drive>\Program Files\Trellix\IPS Manager\App`. For an upgrade, it is the same location as that of the earlier version.
  - Restore Default Folder: Resets the installation folder to the default location.
  - Choose: Browse to a different location.

### Caution

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

### Note

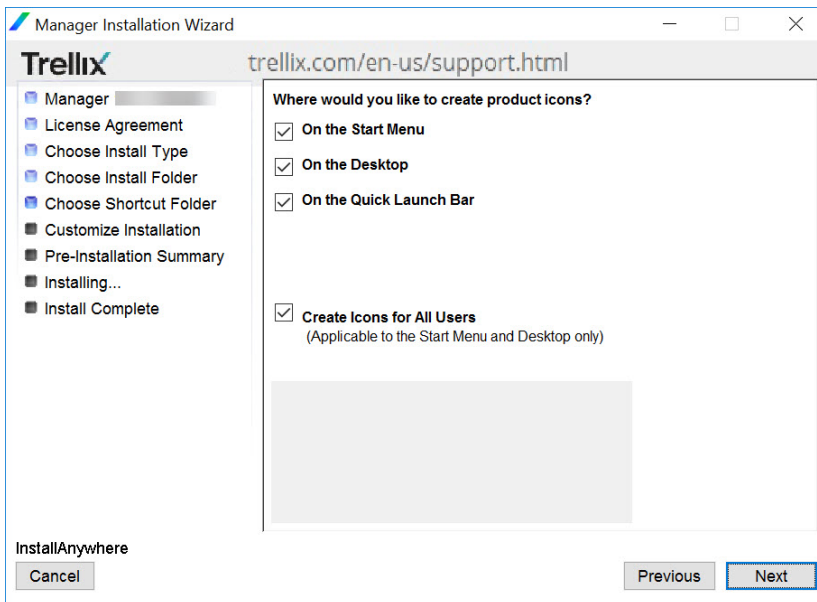
The Manager software cannot be installed to a directory path containing special characters such as a comma (,), equal sign (=), or pound sign (#).



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

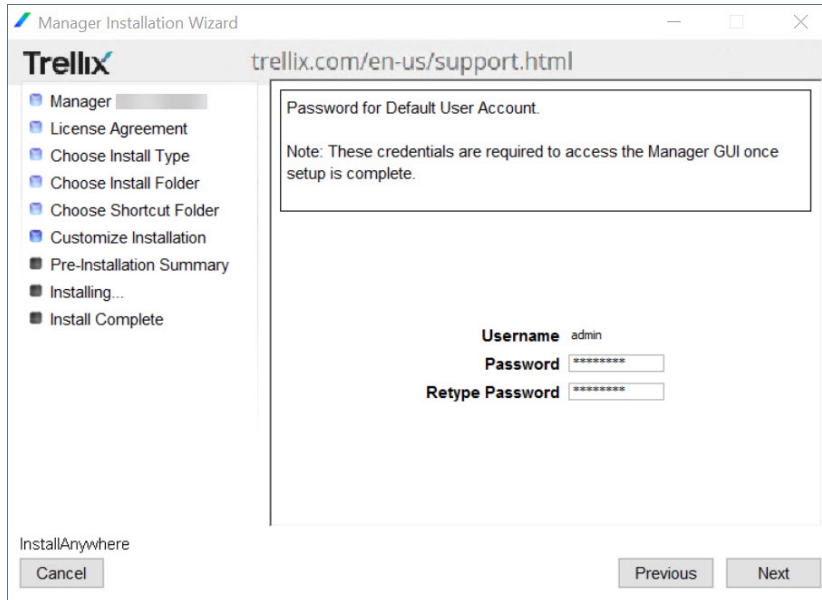
You can include or remove multiple options by selecting the relevant check boxes.



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.

 Note

Trellix strongly recommends that the password must be at least 8 characters in length and must contain a combination of numbers, characters, and special characters. For more information on the password control, see section *Configure password complexity settings* in *Trellix Intrusion Prevention System Product Guide*.



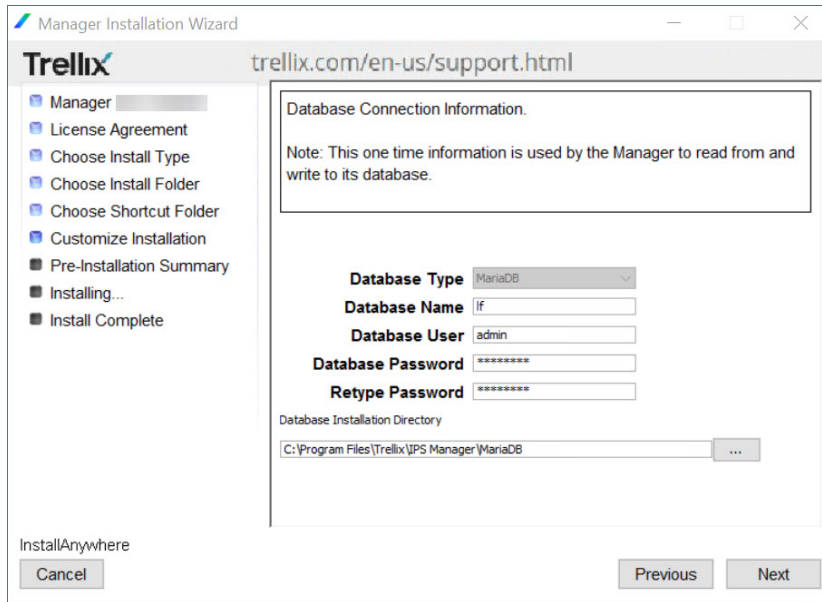
## 8. Set the following:

- Database Type is displayed as MariaDB. You must use only the MariaDB 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 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 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 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.

 Important

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

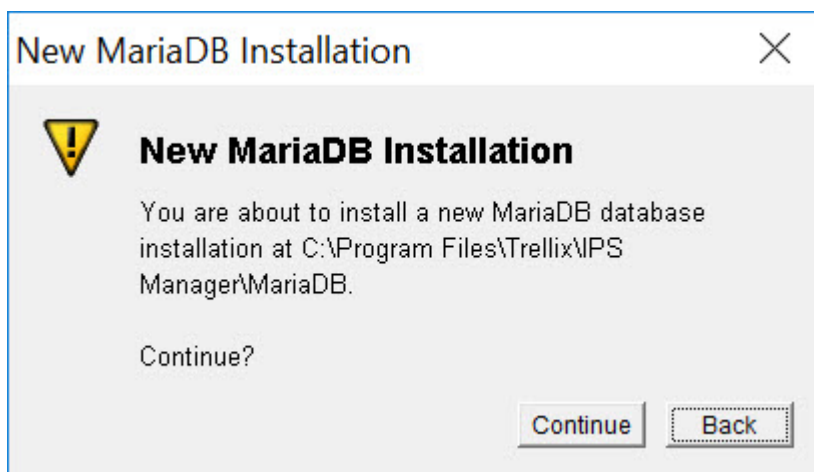
- **MariaDB Installation Directory:** Type or browse to the absolute location of your selected Manager database. For a first-time installation, the default location is: <System\_Drive>\Program Files\Trellix\IPS Manager\MariaDB. You can type or browse to a location different from the default. However, the database must be on the same server as the Manager. For upgrades, the default location is the previous database installation directory. The user names and user permissions will be same as before.



9. Click Next.

### Note

If you are creating a new database, New MariaDB Installation message appears asking to confirm that you really want to create a new database. Click Continue to continue with the installation.

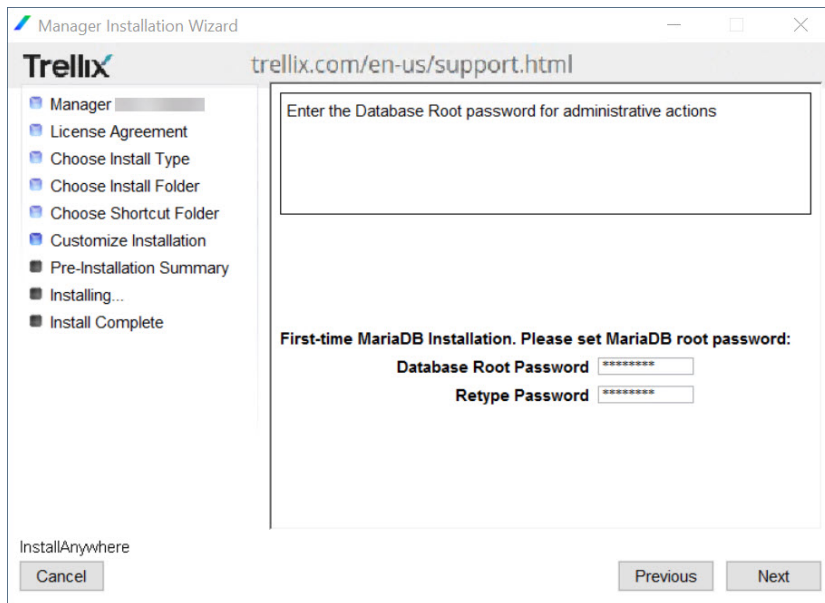


10. Type the root password for your database. If this is the initial installation, type a root password and then type it again to confirm. The MariaDB root password is required for root access configuration privileges for your database. Use a

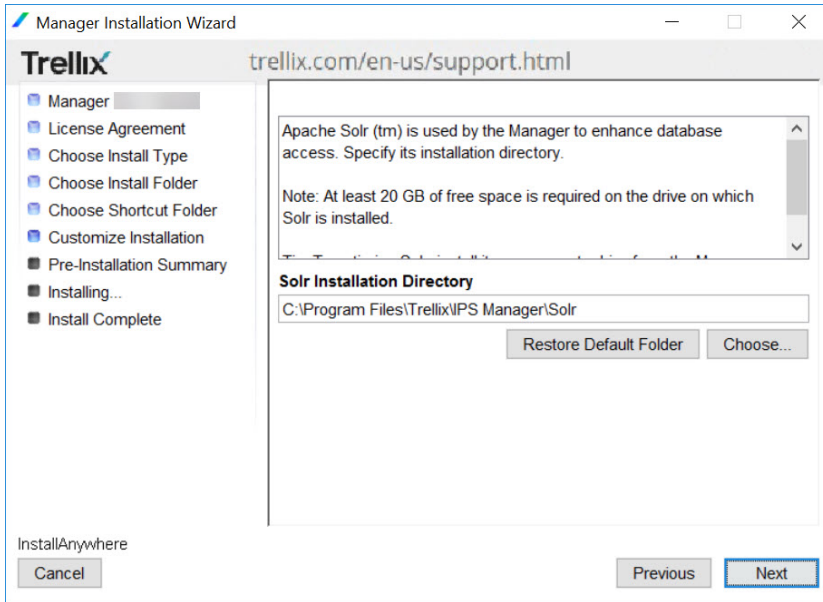
combination of alphabets [both uppercase (A-Z) and lowercase (a-z)], numbers [0-9] and/or, special characters like "~ ` ! @ # \$ % - \* \_ + [ ] : ; , ( ) ? { } ". Do not use null or empty characters.



For security reasons, you can set a MariaDB root password that is different from the Database Password that you set in a previous step.



11. Choose the folder in want 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 <System\_Drive>\Program Files\Trellix\IPS 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.

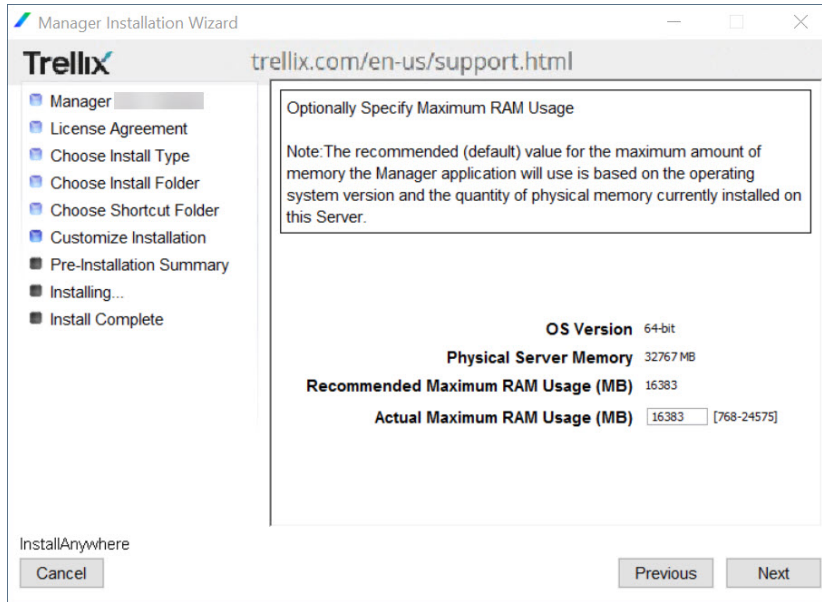
### Note

The Solr installation directory screen will not be displayed during the Central Manager installation.

12. Click Next.

### Note

11.1 Manager installation is supported only on 64-bit OS. If you try installing it 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 Trellix IPS. Since Jboss memory uses hard-disk-based memory (program memory), the total amount of both can exceed the Manager server's RAM memory size.

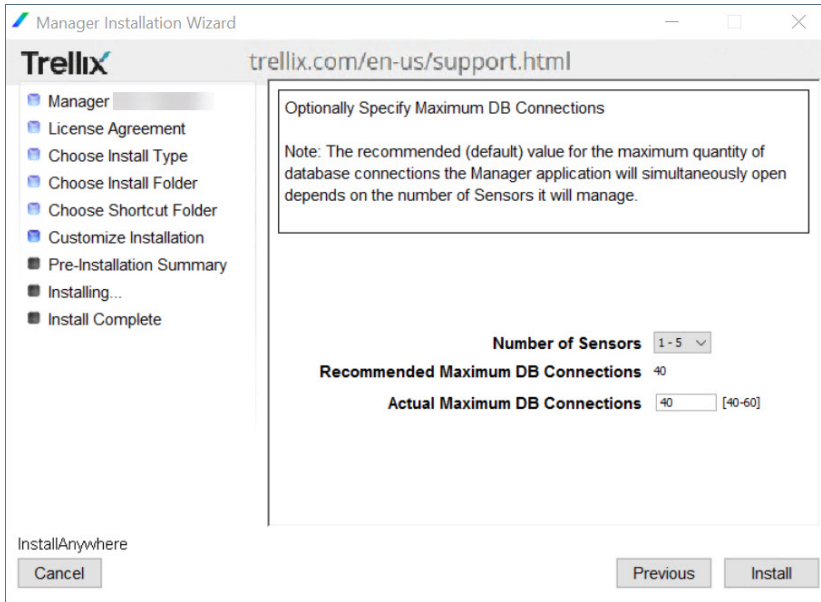
### Note

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 in Trellix IPS Manager):

- Number of Sensors: Select the numbers of IPS 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.



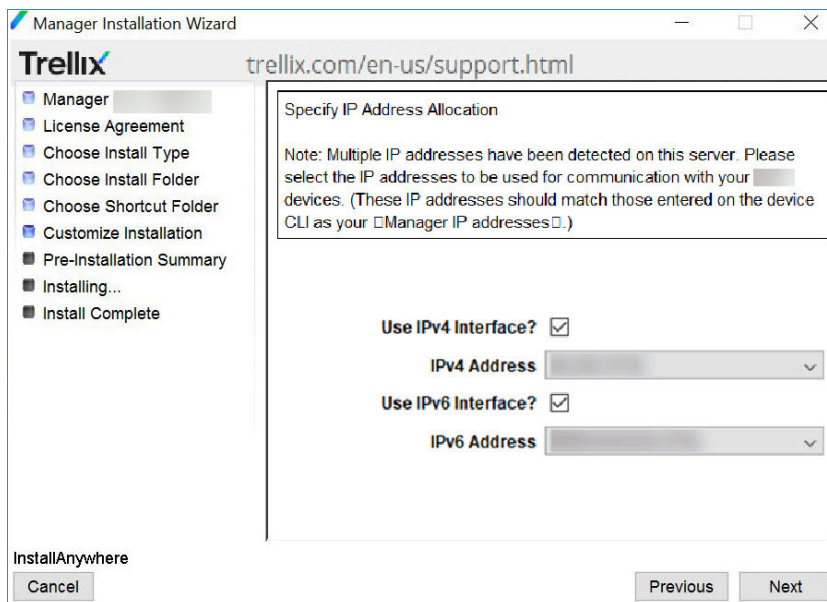


- If the Manager server has multiple IPv4 or IPv6 addresses, you can specify a dedicated address that it should use to communicate with the Trellix IPS devices. To specify an IP address, select Use IPv4 Interface? or Use IPv6 Interface? and then select the address from the corresponding drop-down list.

 **Note**

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 Trellix IPS devices.



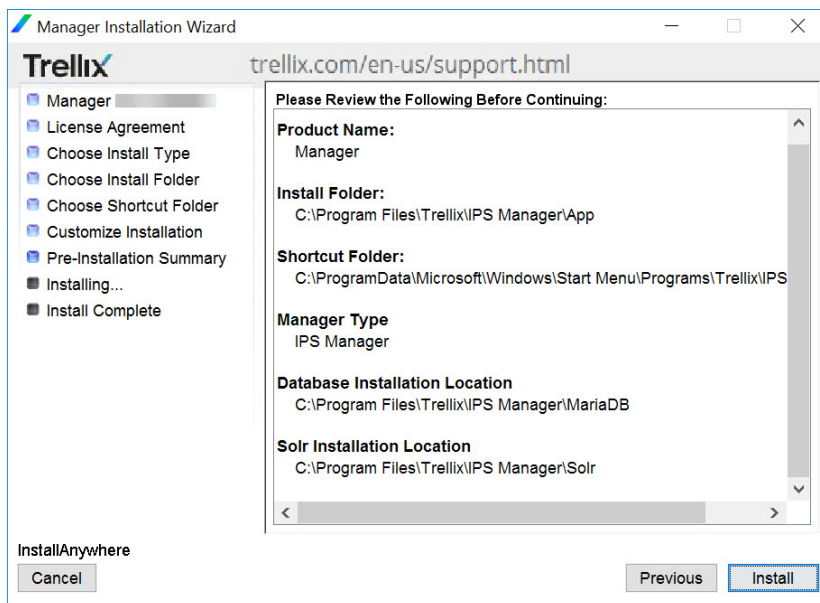
- If the Manager has an IPv6 address, then you can add Sensors with IPv6 addresses to it.

- 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.

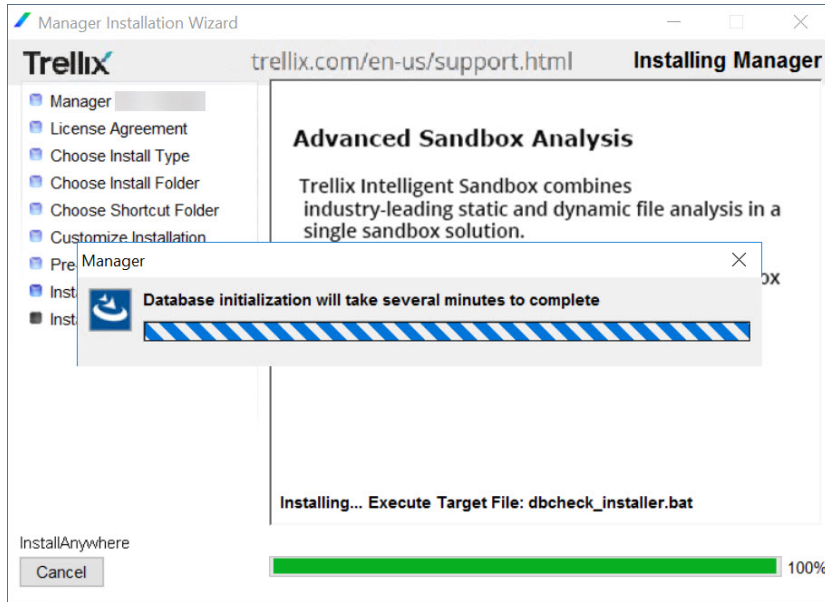
15. In the Manager Installation Wizard, review the Pre-Installation Summary section for accurate folder locations and disk space requirements. This page lists the following information:

- 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 Installation location: The location on your hard drive where the database is to be located, which you specified in Step 8.
- Solr Installation location: The location on your hard drive where the Solr is to be located, which you specified in Step 11.
- 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 database are installed to your target server. In case of an upgrade, database information is synchronized during this process.



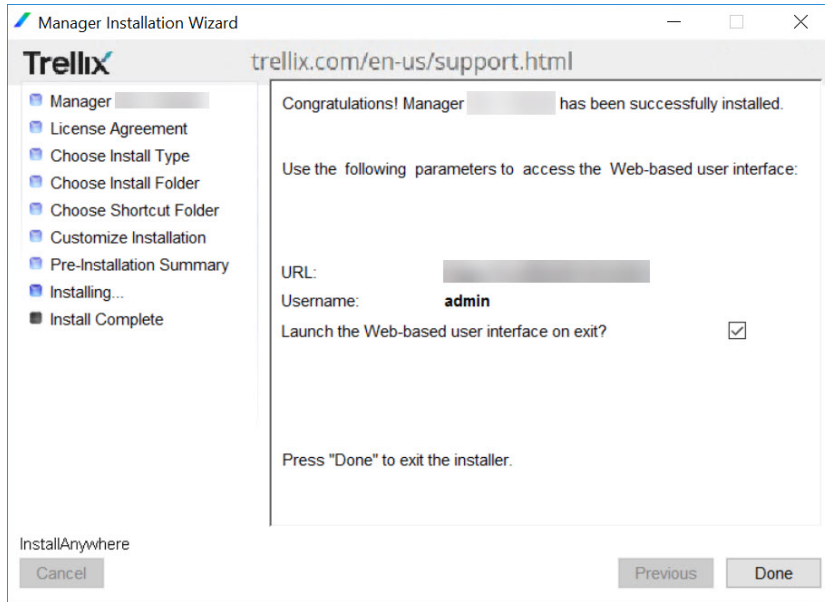
### Important

Post-installation, you can check the `initdb.log` (from `<Manager_Install_Dir>\App\logs`) for any installation errors. In case of errors, contact Trellix Support with `initdb.log`.

17. A congratulatory message appears upon successful installation. The Manager Installation Wizard displays the following fields.

- URL to access web-based user interface. For example, if the Manager server's computer name is Callisto, 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.

### Note

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.

### Note

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

20. Type a valid login ID (default: admin) and password (default: admin123) for Trellix IPS Manager, and login ID (default: nscmadmin) and password (default: admin123) for Trellix IPS Central Manager.
21. You can use the Manager Initialization Wizard to complete the basic configuration steps.

:

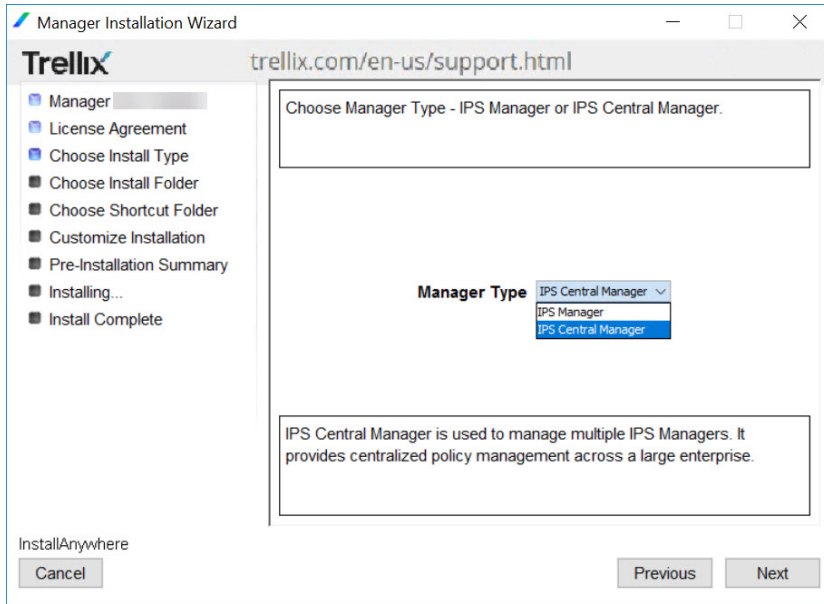
## Installing the Central Manager

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 IPS Central Manager. By default, IPS Manager is selected.

---

Central Manager installation



### Note

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 MariaDB. No centralized database exists in an Central Manager setup.

### Note

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

:

## Launch virtual instance of the Manager on MLOS

The MLOS Virtual Manager image for ESXi and KVM servers allow you to create virtual instances of the IPS Manager/Central Manager running on MLOS. Refer to the sections *Create a Manager instance using OVA file* and *Create a Manager instance using qcow2 file* for creation of virtual instances of the Manager.

:

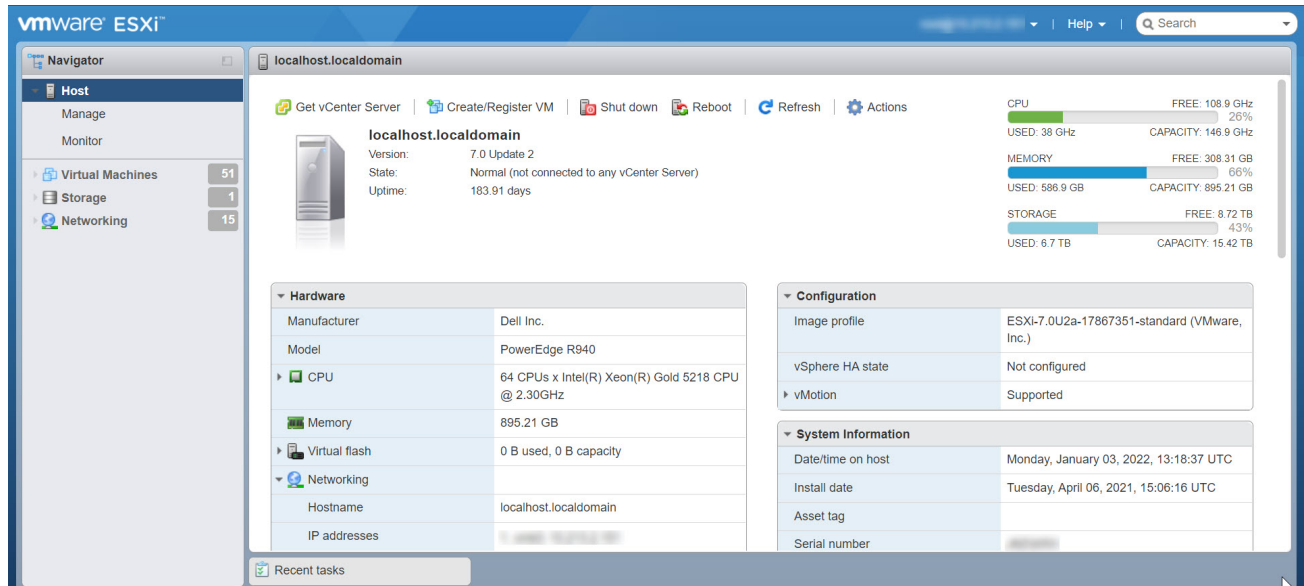
## Create a Manager instance using OVA file

### Prerequisites:

- You should have a Virtual network defined in the ESXi server for management access.
- Make sure you have more than 500 GB disk space available in your ESXi server, as the Linux-based Central Manager/ Manager requires 500 GB disk space.

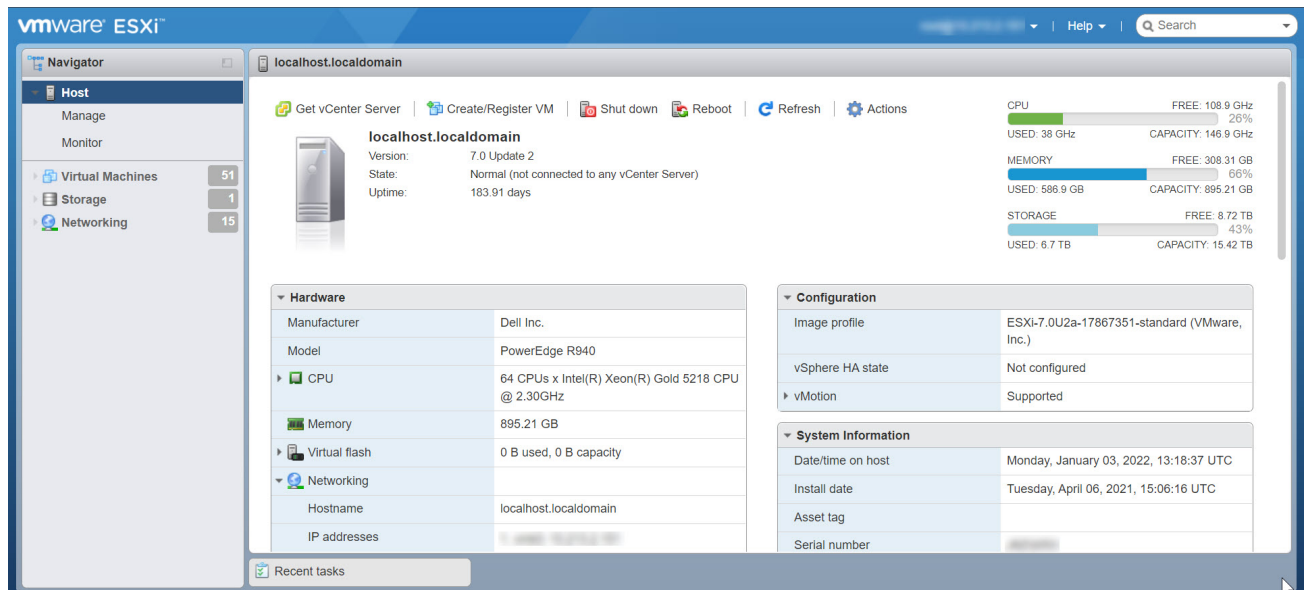
### Steps:

1. Log on to the VMware ESXi server. Select Host menu from the **Navigator** pane.



The Host page is displayed.

2. Select Create/Register VM option.  
The New virtual machine dialog box is displayed.
3. Select Deploy a virtual machine from an OVF or OVA file option and select Next.



The Select OVF and VMDK files section is displayed.

4. In the Enter a name for the virtual machine field, provide the name of the virtual machine.

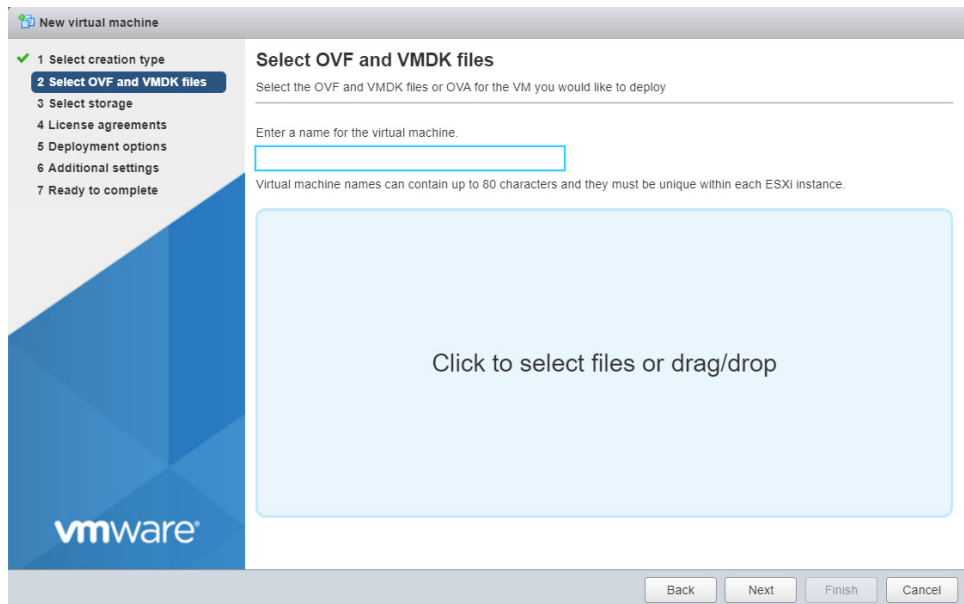
### Note

The name can contain up to 80 characters including alphabets, numerals, and special characters.

Select Click to select files or drag/drop option and navigate to location where the file is placed. Then, select the required Manager OVA file and click Next option.

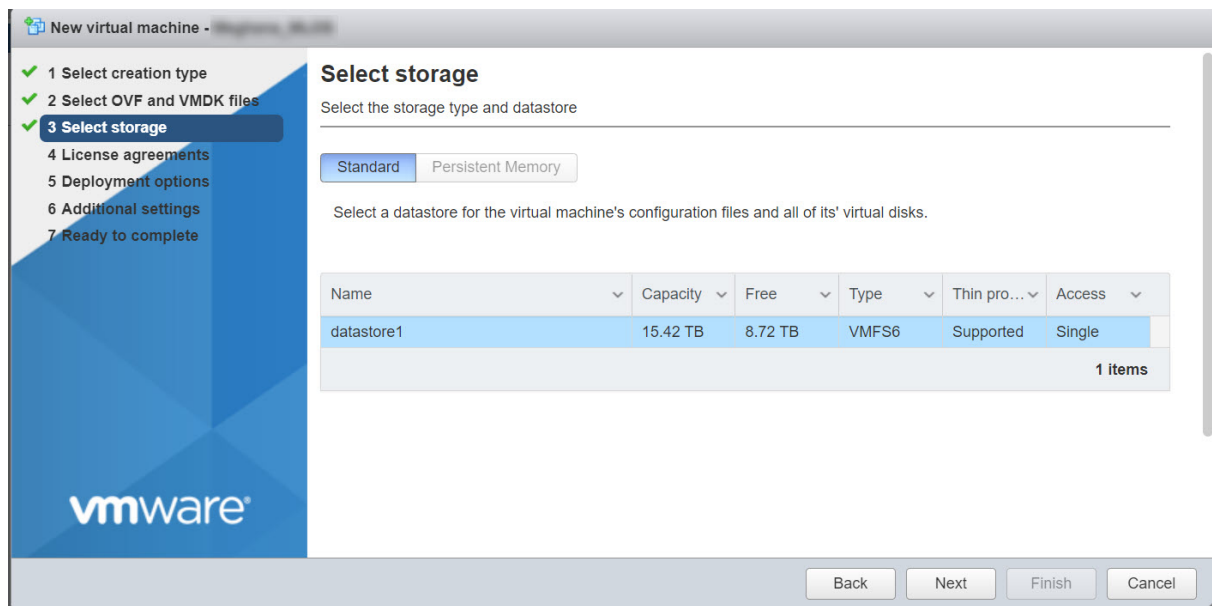
### Note

The Manager and Central Manager uses different OVA file, you can download the required OVA file from the [Download Server](#).



The Select storage section is displayed.

5. Configure the required storage type and datastore for the virtual machine and click Next option.



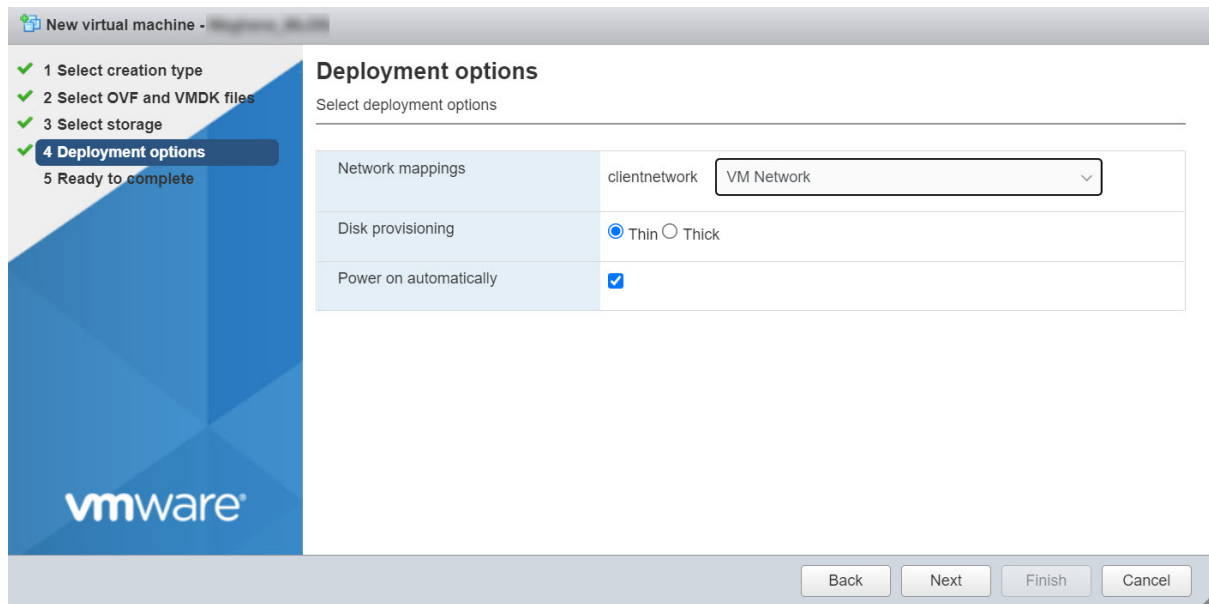
The Deployment options section is displayed.

6. In the Deployment options section, the following options are displayed:



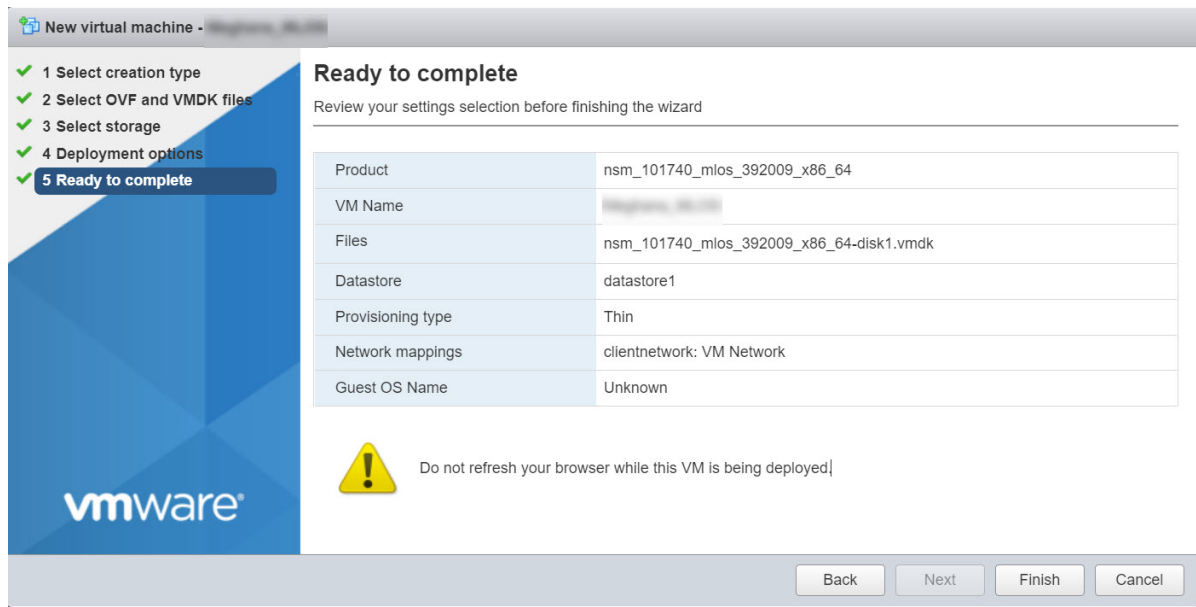
Network mappings	From the Network mappings drop-down, select clientnetwork as VM Network.
Disk provisioning	Choose the Disk provisioning as Thin or Thick depending on the availability of physical disk storage. It is recommended to use the default provision as Thin.
Power on automatically	Enable the Power on automatically option.

After configuring the deployment options, click Next option.



The Ready to Complete section is displayed.

7. Verify the configuration and click Finish to deploy the Linux-based Manager.



8. Once the deployment is complete, you can configure the Linux-based Manager using SSH.

:

### Create a Manager instance using qcow2 file

#### Prerequisites:

- Verify your KVM setup meets the server requirements. See the corresponding sections in [Server requirements](#) and [How to host the Manager on virtualization platforms](#).
- Install KVM on CentOS 7. For installation, refer to the section [Installing KVM on a Linux Machine](#) in *Trellix Virtual Intrusion Prevention System 11.1.x Product Guide*.

#### Steps:

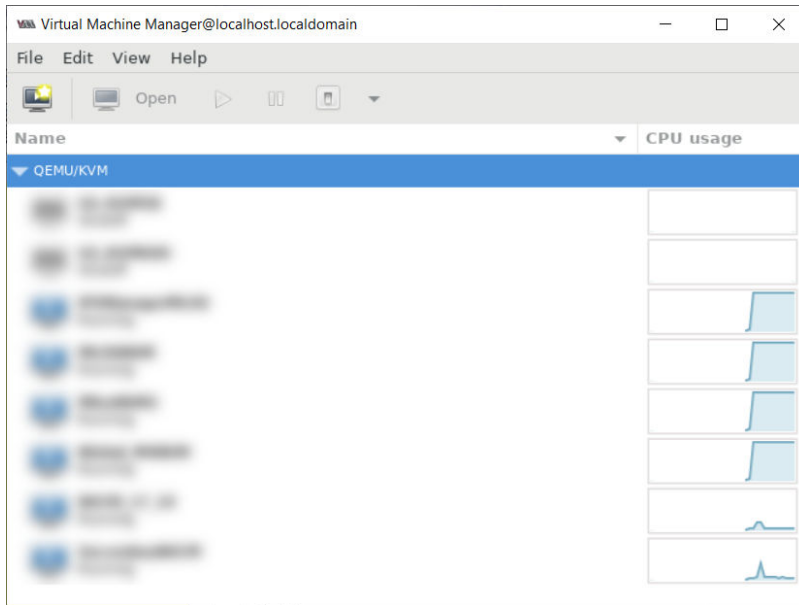
Following steps describe how to install a Linux based Manager/Central Manager through the KVM user interface:


1. Log on to the Linux server user interface using the IP address and the credentials.
2. Launch the virt-manager application by executing the **virt-manager** command through the server's command line terminal.

#### Note

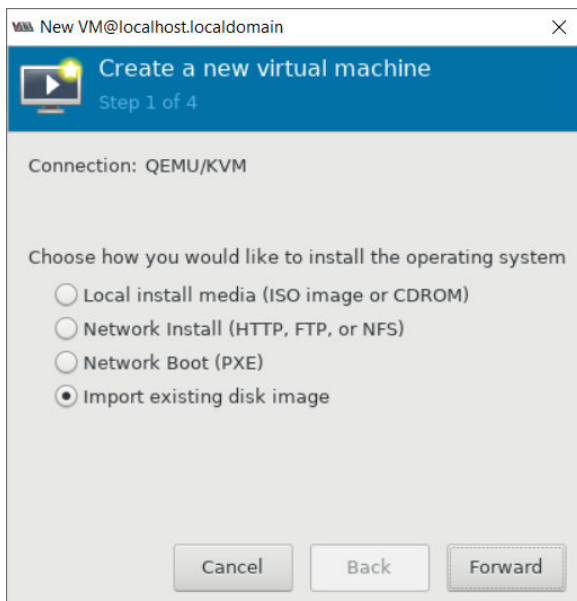
It is recommended to use MobaXterm for remotely accessing the virtual machine manager.

It will direct you to a UI prompt where you can create the required virtual machine. If you have any instances running, you see these instances listed in this window.



3. Click the  icon to create a new virtual machine.  
The Create a new virtual machine wizard window appears.

4. In Step 1 of the wizard, you will be choosing the operating system (OS) installation format and the Architecture. Since you are installing the operating system from an image, you need to select the Import existing disk image radio button.
5. Click Forward to proceed to Step 2 of the wizard.

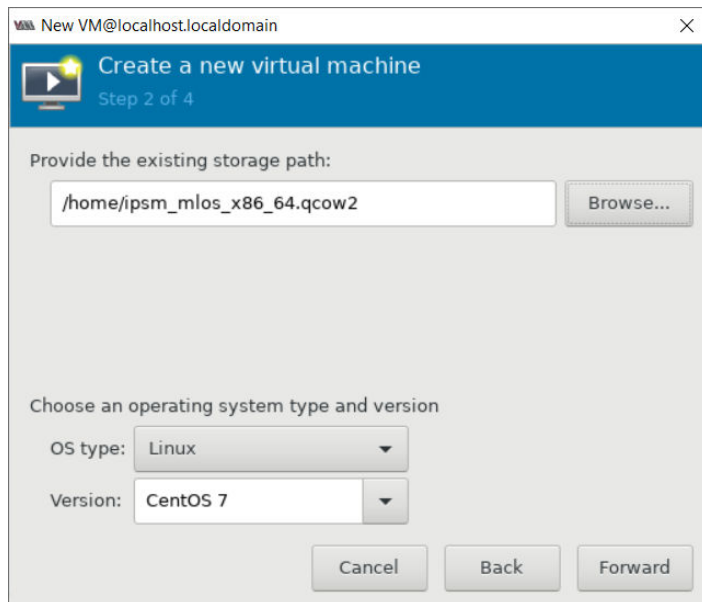


In Step 2, you will be setting the:

- Path where the image file is located
  - OS type
  - OS Version
6. From the OS type drop-down list, select Linux.
  7. From the Version drop-down list, select CentOS 7.
  8. Browse to the location where the Linux based Manager image is placed and select the .qcow2 image. Upon selecting the image, click Forward.

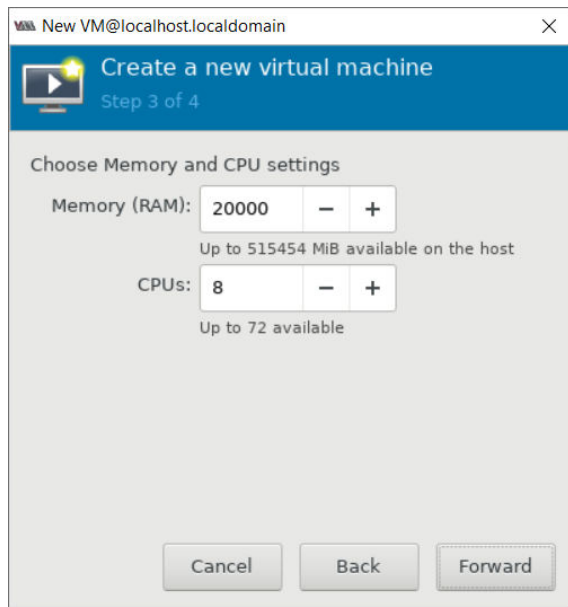
### Note

Trellix recommends that you place the software image in a folder other than the root folder.

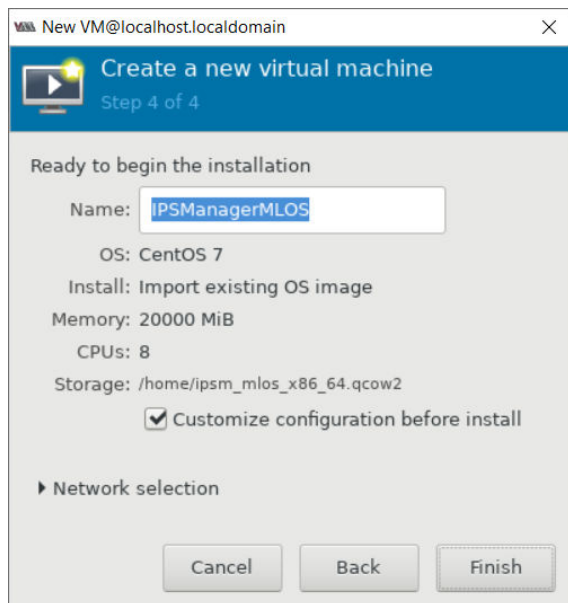


You come to Step 3 in the deployment where you will be setting the memory and CPU requirements for the Manager.

9. Manually enter the Memory (RAM) and the number of CPUs required. The minimum required RAM is 20 GB and the number of CPUs is 8.
10. Click Forward to proceed to Step 4.

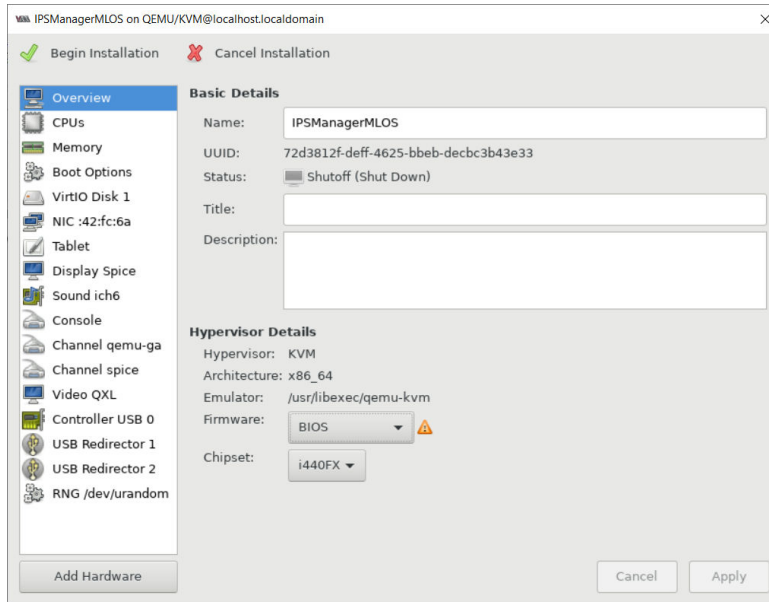


11. In Step 4 of the wizard:
  - a. Enter a name for the Manager.
  - b. Select the Customize configuration before install checkbox.
12. Click Finish to apply all the changes.

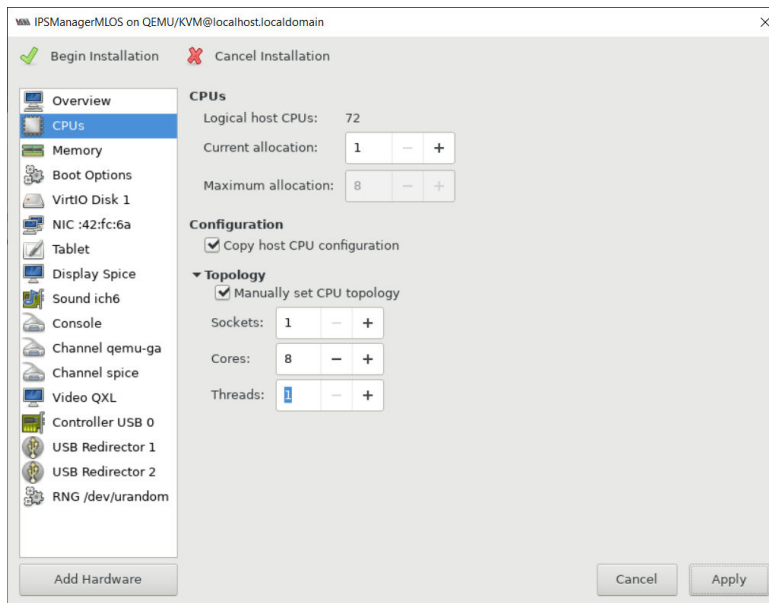


You are routed to the next step in the deployment where you can review the entire configuration tab-by-tab.

13. The configuration wizard appears with the Overview tab selected by default. This tab displays the basic configuration details of the VM.
  - a. Make sure that the Hypervisor is KVM and the Architecture is x86\_64.
  - b. From the Firmware drop-down list, make sure BIOS is selected.

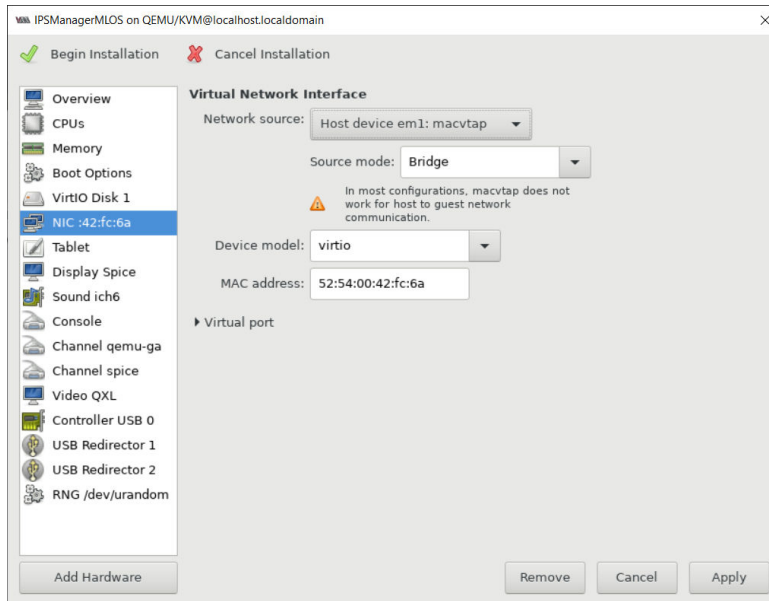


14. Click the CPUs tab.
  - a. Expand Topology, select the Manually set CPU topology checkbox and make sure that the number of Sockets is 1, Cores are 8, and Threads is 1 for better performance.
  - b. Click Apply to confirm your changes.



15. Click the NIC tab.

- a. From the Network source drop-down list, choose the required network interface, leave the other options set to default values and click Apply.



16. Click Begin Installation to deploy the Linux-based Manager.

Creation of the virtual machine begins. This process takes a few minutes. Once deployed, you can configure the Linux-based Manager using SSH.

:

### Dual NIC support in Linux based Manager

The Linux based Manager supports dual NIC. It means you can configure both public and private IP addresses to the Linux based Manager.

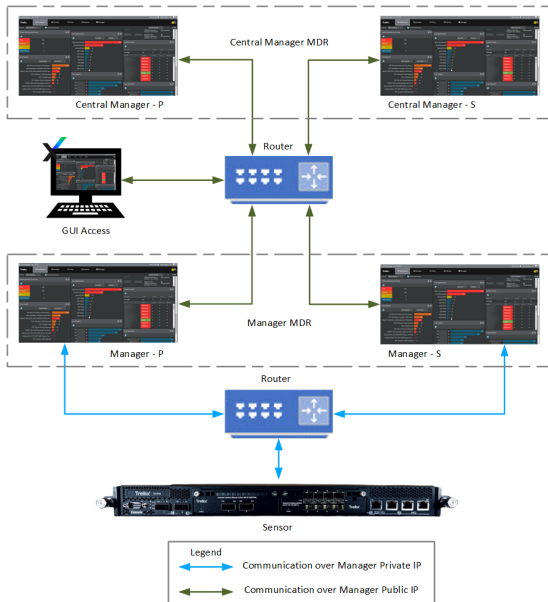
You can configure the public and private IP addresses to the NIC interfaces using **set network configuration** command in the Manager shell.

#### Considerations:

- The private IP address is for Manager-Sensor and MDR communication. Therefore, you must configure the MDR pair using the private IP address.
- Dual NIC is not supported in the Linux based Central Manager.
- The Manager and Central Manager communication is supported over the Public IP address only. Therefore, you must configure the Trellix Intrusion Prevention System Central Manager using the public IP address.
- The Manager GUI is accessible using the public IP address.

## 1 | Installing Trellix Intrusion Prevention System

Consider a Linux based Manager deployment configured with dual NIC. The Manager here is in an MDR pair and managed by a Trellix Intrusion Prevention System Central Manager in an MDR pair. In this scenario, the Manager MDR pair and Manager-Sensor communication take place over the private IP address, whereas the public IP address is used for the Manager-Central Manager communication and GUI accessibility.



:

### Configure the Manager on MLOS

#### Steps:

1. Log in to the Manager shell using the following credentials:

- Username: **admin**
- Password: **MLOSnmApp**

#### Note

SSH connection to the Linux based Manager Appliance is not supported by Putty application. Trellix recommends you to use Tera Term application for remotely accessing the Manager Appliance using SSH.



### Note

Trellix strongly recommends that you change the password immediately. The new password must be at least 8 characters in length and must contain a combination of numbers, characters, and special characters. For more information on the password control, see section *Configure password complexity settings* in *Trellix Intrusion Prevention System Product Guide*.

2. To update network parameters, execute the **set network configuration** command. Syntax: **set network configuration**

### Note

The **set network configuration** command overwrites the pre-existing network configuration in the Manager server.

### Note

You can only configure IPv4 addresses in the MLOS Manager Appliance box.

### Note

You can terminate the network configuration by executing the **quit** command.

On executing the **set network configuration** command, follow the steps below:

- a. Select the type of NIC configuration:

```
Please select one of the below option: 1 -> Configure Single NIC 2 -> Configure Both the NIC's
Input 1 or 2 based on you selection :
```

Type **1** to configure NIC 1 or NIC 2, or **2** to configure both NIC 1 and NIC 2.

- b. Select the NIC to be configured with public IP address for management purpose:

```
Enter the NIC you want to configure with public network ip: 1 -> eth0 [NIC 1] 2 -> eth1 [NIC 2]
Input 1 or 2 based on your selection :
```

Type **1** to select NIC 1 or **2** to select NIC 2 based on your network cable connection for public IP address.

### Important

The NIC 1 and NIC 2 ports are interchangeable:

- When configuring a single NIC, you can assign the public IP address to NIC 1 or NIC 2.
- When configuring dual NIC, you can assign a public IP address to NIC 1 and a private IP address to NIC 2 or vice-versa.

### Note

The Manager Appliance can have only one public and one private IP address.

c. Enter the Manager Appliance network parameters as shown below:

Parameters	Description
<b>DOMAIN NAME</b>	Enter the domain name for the Manager server.
<b>HOSTNAME</b>	Enter the hostname to be assigned to the Manager server.
<b>Configuring the eth"x" with public IP</b>	
<b>IP ADDRESS</b>	Enter the public IP address to be assigned to the Manager server.
<b>NETMASK</b>	Enter the subnet mask for the Manager server.
<b>GATEWAY</b>	Enter the gateway address for the Manager server.
<b>DNS1</b>	Enter the primary DNS server IP address.
<b>Do you want to enter DNS2 &lt;y/n&gt;</b>	Type <b>y</b> , if you want to configure a secondary DNS server IP address, else type <b>n</b> .
<b>DNS2</b>	(Optional) Enter the secondary DNS server IP address.
<b>Configuring the eth"y" with private IP</b> (Applicable only when <b>2 -&gt; Configure Both the NIC's</b> option is selected in step a).	
<b>IP ADDRESS</b>	Enter the private IP address to be assigned to the Manager server.

### Note

The Manager server will reboot automatically after completing the network configuration.

### Note

Make a note of the MAC address displayed after successful execution of **set network configuration** command.

You can now use the public IP address to access the UI from a remote location using a client machine and manage the Manager Appliance from a remote location using SSH . If required, unplug the monitor, keyboard, and mouse.

:

## Log files related to Manager installation and upgrade

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

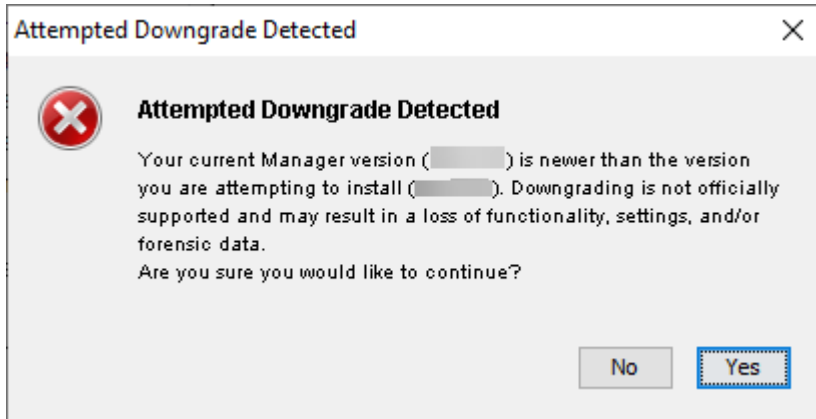
- **mgrVersion.properties:** Every fresh installation or upgrade of the Central Manager or Manager is logged to this file. Each entry contains the version of the Central Manager or Manager that you installed or upgraded to. It also contains the date and time of when you performed this action. This can 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. The purpose of 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\logs. 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 on both Windows based Manager and Linux based Manager. 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 for Windows based Manager.

---

Attempted Downgrade Detected dialog



:

### Product Registration

The Manager should be registered with Trellix for receiving automatic updates regarding the signature set, callback detectors, and device software from Trellix in real time.

At a higher level, the Manager registration with Trellix is a two-step procedure as follows:

1. Obtain the Trellix IPS Registration Key from Trellix.
2. Register the Manager instance with Trellix using the Trellix IPS Registration Key.

Trellix recommends you to register the product immediately after installation when the Product Registration window appears after the initial login.

Upon skipping product registration, the following functionalities will be disabled:

- On-demand and scheduled download of Signature Sets in the Manager
- On-demand and scheduled download of Callback Detectors in the Manager
- On-demand download of device software
- Creating vIPS Components and vIPS Protected Groups

On registering the Manager with Trellix, some threat and device-specific data will be sent to Trellix telemetry servers at different intervals when Telemetry is enabled. If, at any point, you want to review the telemetry data you are sending to Trellix, run the required Default - Telemetry Next Generation report from the Analysis → <Admin Domain Name> → Even Reporting → Next Generation Reports page.

#### Note

Telemetry is enabled in the Manager by default. You can change the telemetry configurations from Manager → <Admin Domain Name> → Setup → Telemetry page. Refer to the *Telemetry* section in *Trellix Intrusion Prevention System Product Guide* for more information.

:

### Obtain the Trellix IPS Registration Key

To obtain the Trellix IPS Registration Key, perform the following steps:

1. Go to the [Trellix Download Server](#).
2. Login using your Grant Number and registered Email Address.

#### Note

If you do not have a Grant Number provided by Trellix, contact [Trellix Technical Support](#) and request for a trial Grant Number.

The My Products page opens.

3. Make a note of the Trellix IPS Registration Key.

#### Note

The Trellix IPS Registration Key is unique to each customer. For example, if Customer A has two grant numbers, 1234 and 5678, the Trellix IPS Registration Key is the same for both of these grant numbers as the registration keys are generated per customer.

:

### Register the IPS Manager with Trellix

To register your Manager with Trellix, do the following:

#### Prerequisite:

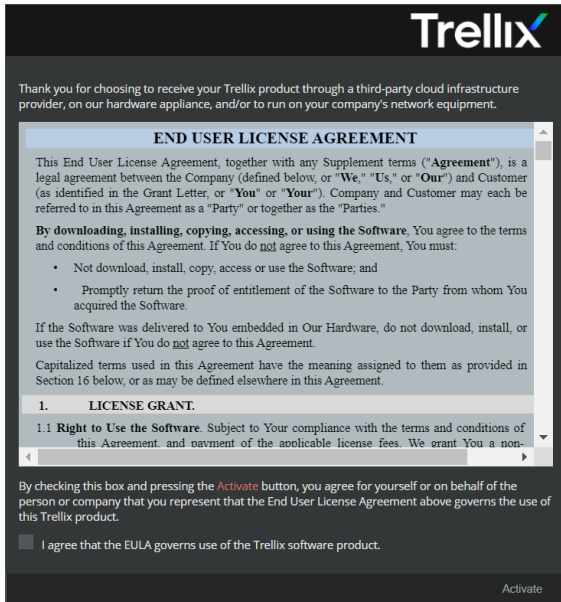
Obtain the Product Registration Key from the [Trellix Download Server](#).

#### Note

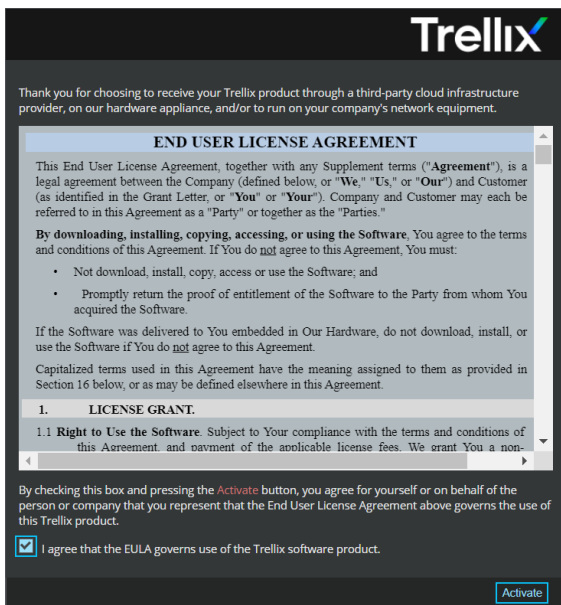
If you have skipped the Product Registration during initial login after installation or upgrade, go to Manager → <Admin Domain Name> → Summary (Manager → Summary in Central Manager), click Register Product, and follow the below procedure from step 3 to register the Manager.

#### Steps:

1. Log in to the Manager. The End User License Agreement opens.



2. Select the checkbox and click Activate.



### Note

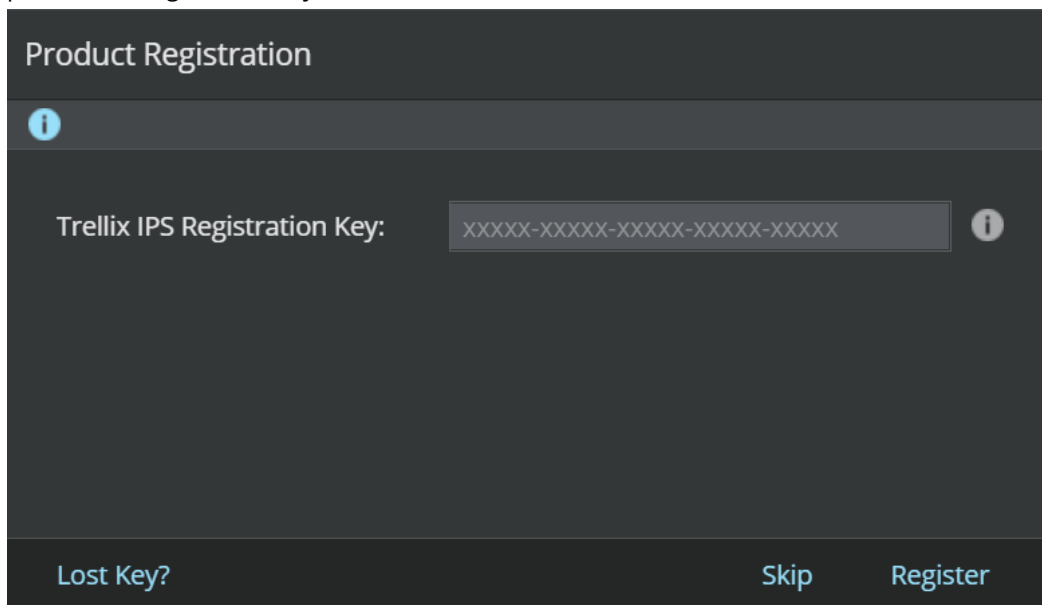
Trellix recommends you perform Product Registration immediately after the initial login. If you do not want to register the Manager, click Skip.

 **Note**

When the Manager is not registered with Trellix, the following features are automatically disabled:

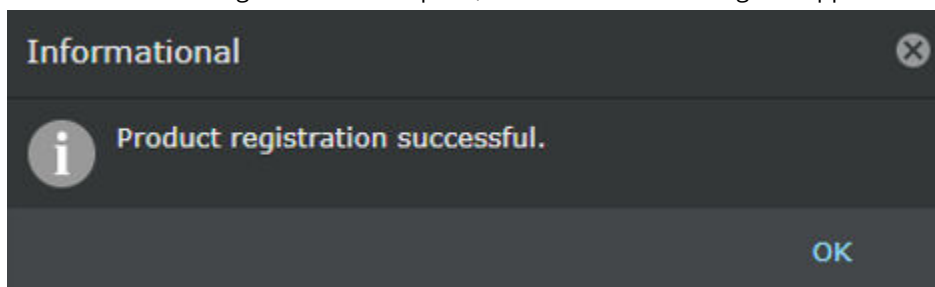
- Download Signature Sets
- Download Callback Detectors
- Download Device Software
- Signature Sets Automatic Updating
- Callback Detectors Automatic Updating

3. The Product Registration dialog box appears. In case you do not have the registration key readily available, click Lost Key? to procure the registration key.



4. Enter the Trellix IPS Registration Key and click Register.

5. Once the Product Registration is complete, an Informational dialog box appears with success message.



:

## Starting the Manager/Central Manager

This section assumes you have permissions granting you access to the software. In Trellix Intrusion Prevention System, 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 the Trellix IPS. 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 Trellix Intrusion Prevention System Super User.

### Important

For testing purposes, you can access the Manager from the server. For working with the Manager/Central Manager, Trellix 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:

#### Steps:

1. Make sure the following services are running on the Manager server:

- Trellix IPS Manager
- Trellix IPS Manager Database
- Trellix IPS Manager Watchdog

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:

- Trellix IPS Central Manager
- Trellix IPS Central Manager Database
- Trellix IPS Central Manager Watchdog

Start the services using one of these methods to start the Windows based Manager, Database, and Watchdog services:

- Select Start → Settings → Control Panel. Double-click Administrative Tools, and then double-click Services. Locate the services starting with Trellix IPS 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.

Start the Linux based Manager, Database, and Watchdog services by executing the following commands in the Manager shell:

- Execute the **manager start** command to start the Manager/Central Manager service.
- Execute the **database start** command to start the Manager/Central Database service.
- Execute the **watchdog start** command to start the Manager/Central Watchdog service.

2. Open the Manager

- Server - Double-click the shortcut icon that you created during installation.
- Client machine - Start your browser (Internet Explorer 11.0, Microsoft Edge 44.0, Mozilla Firefox 20.0, or Google Chrome 76.0) 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.



### Note

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.

:

### CA-signed certificate for the Web Server Authentication

The Manager/Central Manager use self-signed certificate to establish a trusted connection with the client systems. You can also use a CA-signed certificate issued by trusted CAs, such as Verisign, GeoTrust, and others, to establish trust between the Manager server and the client systems.

:

### Considerations for CA-signed certificate for the Web Server Authentication

The CA-signed certificate for the Manager is considered valid if the following conditions are met:

- The certificate must be X.509v3 version.
- The CA-signed certificate chain should comply with the following requirements:
  - Should be issued from a trusted Certificate Authority
  - Should be in P12 format
  - Must contain valid serial numbers and valid issuer domain name
  - Must include minimum SHA256 with RSA 2048 bit encryption
- Ensure that the validity period for the certificate specifies a valid date range.

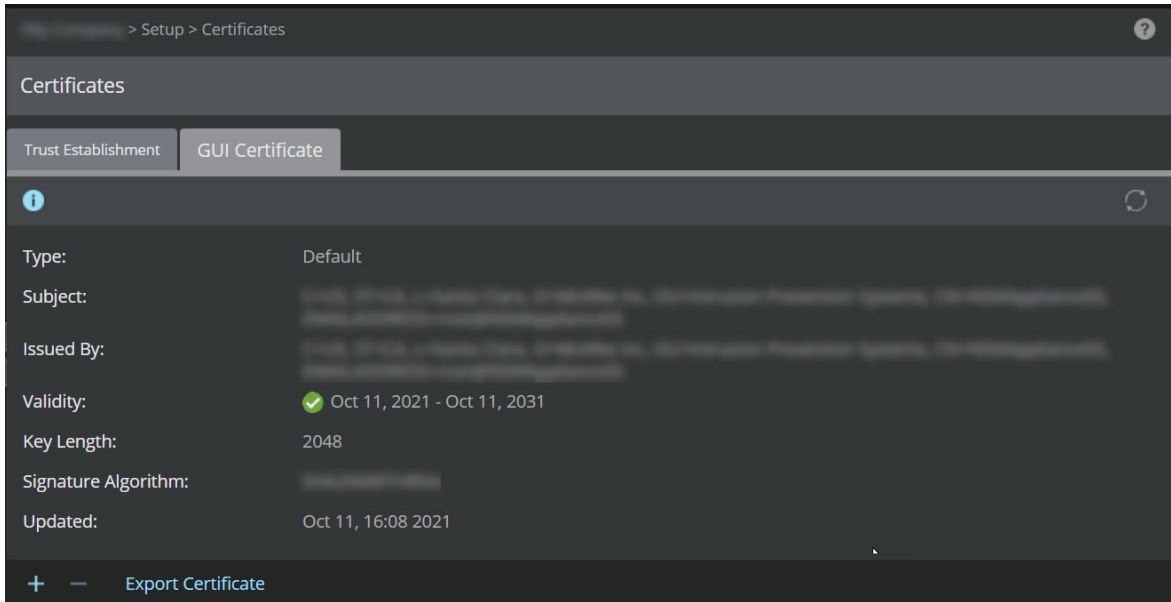
:

### Import the CA-signed certificate for Web Server Authentication

To import the CA-signed certificate to the Manager, perform the following steps:

#### Steps:


1. In the Manager, go to Manager → <Admin Domain Name> → Setup → Certificates. Select GUI Certificate tab. The GUI Certificate tab is displayed.



2. Click .

The Import Certificate dialog box opens.

### Note

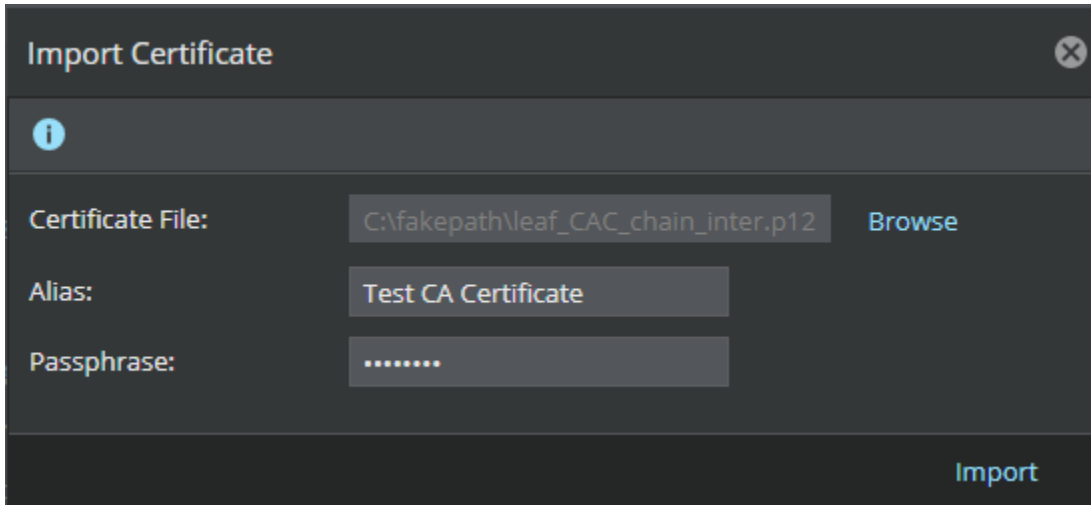
The  option is available only when the Manager uses a self-signed certificate. You cannot add a new CA-signed certificate to the Manager that is already using a CA-signed certificate for establishing trust with the client systems.

3. In the Import Certificate dialog box, click Browse.

4. Browse to the directory that contains the CA-signed certificate, click Open.

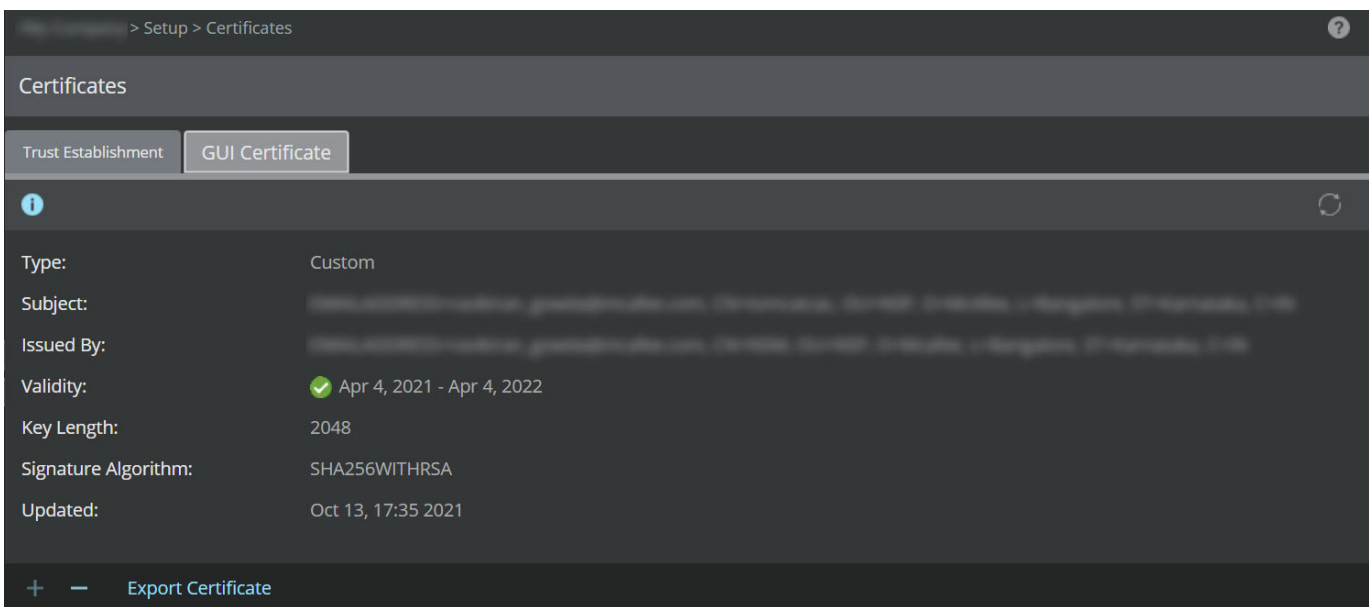
### Note

The CA certificate should be in P12 format.



5. Provide an Alias and the Passphrase of the certificate.
6. Click Import to upload the certificate to the Manager.
7. Restart the Manager server.

The Manager server starts to use the CA signed certificate to establish trust with the client systems.



:

## Export the CA-signed certificate for Web Server Authentication

To export the CA-signed certificate from the Manager, perform the following steps:

### Steps:

1. In the Manager, go to Manager → <Admin Domain Name> → Setup → Certificates. Select GUI Certificate tab.

The GUI Certificate tab is displayed.

2. Click Export Certificate and save the file to a location of your choice.


:

### Delete the CA-signed certificate for Web Server Authentication


To delete the CA-signed certificate from the Manager, perform the following steps:

#### Steps:

1. In the Manager, go to Manager → <Admin Domain Name> → Setup → Certificates. Select GUI Certificate tab. The GUI Certificate tab is displayed.

2. Click . The Confirmation dialog box opens.

#### Note

The  option is available only when there is a CA-signed certificate in the Manager. You cannot delete the self-signed certificate in the Manager.

3. Click OK to confirm deletion.

#### Note

When the CA-signed certificate in the Manager is deleted, automatically a self-signed certificate is used for the web server authentication.

4. Restart the Manager server. The Manager server automatically starts using self-signed certificate to establish trust with the client systems.

:

### Authentication of access to the Manager using CAC/PIV

Common Access Card (CAC) and Personal Identification Verification (PIV) are smart cards that are used for general identification as well as authentication of user access to secure networks. CAC/PIV holds a unique digital certificate and user information, such as photograph, personal identification number (PIN), and signature, to identify each user. Trellix IPS provides an option for authentication of users to log onto the Manager based on their smart card verification.

Authentication to the Manager using CAC/PIV requires a smart card reader connected to the Manager client workstation. The administrator inserts the CAC/PIV into the smart card reader and opens the Manager UI through the web browser. The Manager

sends an SSL certificate to the client and requests the user's certificate from the browser. The browser validates if the Manager's certificate is signed by a trusted Certificate Authority. The browser then selects the user's certificate by prompting the user if required. The browser retrieves the selected certificate from the smart card which triggers the CAC/PIV interface software (called middleware) to request the user PIN associated with the smart card. The user must correctly enter the PIN to unlock the smart card.

The Manager validates the following attributes of the user's certificate:

- If the certificate is signed by a trusted Certificate Authority (CA)
- If the certificate is valid and has not been revoked
- When the certificate was last validated

The Manager extracts the common name from the user's certificate and checks for a matching administrator account in the Manager with that common name. If the match is successful, a secure session is established and the user is logged into the Manager.

To validate the user's certificate, the trust chain is validated by two CA certificates. The first validation is that the client's certificate is signed by the intermediary CA. Then the intermediary CA certificate is validated by verifying if it was signed by the root CA which is trusted. The root CA is a self-signed CA that is used to sign the intermediary CA certificates.

At a high level, authenticating user access to the Manager through CAC/PIV can be brought about by a 5-step process:

- Obtain the CA certificates
- Import the CA certificates
- Set up CAC users in the Manager
- Enable the CAC authentication
- Log on to the Manager using the CAC/PIV authentication

:

### Obtain the CA certificates

Obtain the intermediate and root certificates in the certificate chain of your CAC cards. To obtain the CAC certificates, perform the following steps:

#### Steps:

1. Plug in the CAC card reader in the Windows client machine which is used to access the Manager. The drivers for the smartcard reader are automatically installed and detected. If the drivers are not installed automatically, you have to manually install the drivers for the smartcard reader. To troubleshoot problems with CAC card reader installation, see [Installing and updating the CAC reader driver/Firmware update/Check services to make sure Smart Card is running](#).
2. Once the CAC card reader is active, plug in the CAC card.
3. In the Internet Explorer browser, navigate to Internet Options → Content → Certificates → Personal. The certificates of the card are available in the Personal tab. There are three certificates corresponding to the card's user, two for email and one for ID.
4. Select the certificate for ID and click View.

The Certificate window with the details of the certificate opens.

5. The Certification path tab lists the chain of the certificate.
6. Select the intermediate certificate which is the issuer of the leaf and click View Certificate to view the intermediate certificate.
7. Go to the Details tab in the Certificate window and click Copy to File. This allows you to export the certificate. Choose any of the .cer formats and save it to a file. Trellix recommends you to select Base-64 encoded option as it is compatible with the Manager. Create a new folder for the certificates as "Saved intermediate and root certificates".
8. Repeat the process for the root certificate and save that to a file as well.

### Note

The root and intermediate certificates can be obtained simultaneously by obtaining the certificate chain.

9. Convert the certificates to .pem format and save them in a separate file.

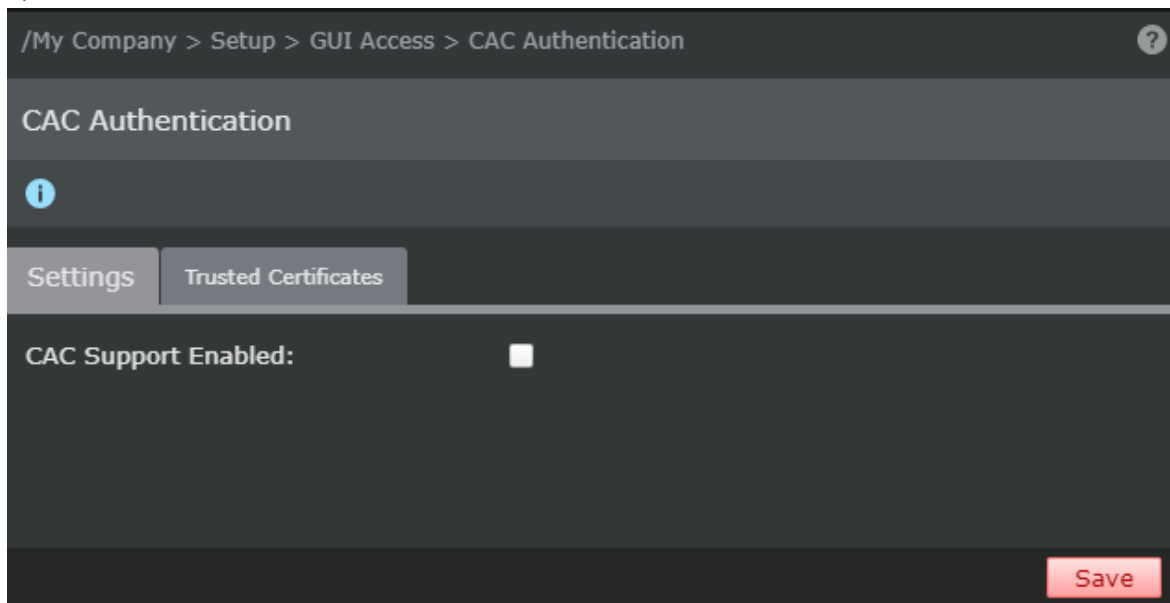
:

## Import the CA certificates

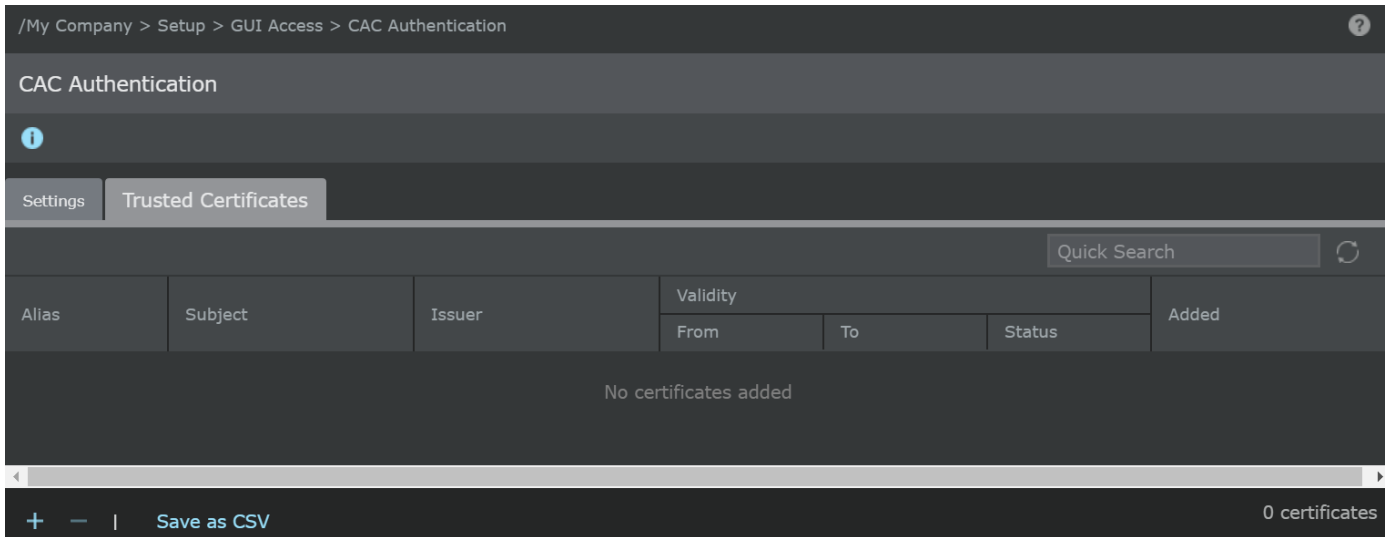
Import the intermediate and root certificates in the certificate chain of your CAC cards to the Manager. To import the CAC certificates, perform the following steps:

### Steps:

1. Log in to the Manager GUI.
2. Go to, Manager → <Admin Domain Name > → Setup → GUI Access → CAC Authentication. The CAC Authentication page opens.



3. In the Trusted Certificates tab, click .



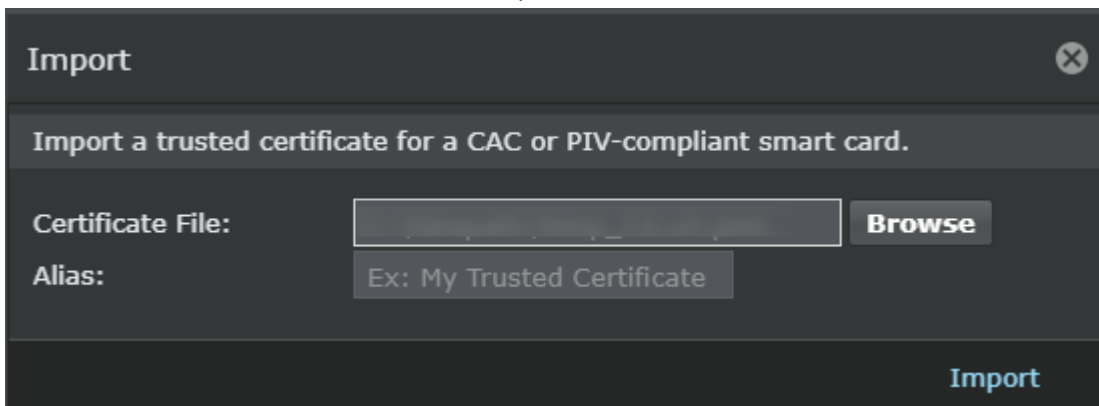
4. In the Import dialog box, click Browse.


5. Browse to the directory that contains the certificate chain and click Open.

 **Note**

The CAC certificate should be in .pem format.

6. Provide an Alias for the certificate and click Import.



7. Click . The Manager imports the certificate to its keystore and the details of the certificate are displayed on the Trusted Certificates tab.

/My Company > Setup > GUI Access > CAC Authentication

### CAC Authentication

Settings Trusted Certificates

Quick Search

Alias	Subject	Issuer	Validity			Added
			From	To	Status	
cacCert	CN=DOD JITC ID CA-...	CN=DOD JITC Root C...	Jan 6, 2017	Jan 7, 2023	Valid	Nov 13, 16:13 2019

+ - | Save as CSV 0 certificates

#### Note

Click Save as CSV to export the trusted certificates details as .csv file.

:

## Set up CAC users in the Manager

### Steps:

1. Connect the smart card reader to your Manager client through a USB port. The smart card reader can be connected to a Manager server, if the server doubles up as a Manager client.
  - Refer to the card reader manufacturer's recommendations for the necessary device drivers to be installed.
  - Install the ActivID ActivClient CAC software on the Manager client.

#### Note

Trellix currently supports integration with smart card reader model SCR3310 from TxSystems. Other smart card readers will also work but have not been tested by Trellix.

2. Insert a card into the card reader.
3. Open the ActivClient software → Smart Card Info → User Name. User name is available in the CN field under Subject in the Certificate details window. The user name is a combination of alphanumeric characters and a few special characters like "." or spaces. For example, "BROWN.JOHN.MR.0123456789"
4. Log onto the Manager and create a user with the exact same name as provided in the CN field, that is "BROWN.JOHN.MR.0123456789".



### Note

If you have RADIUS/LDAP servers in your setup for external authentication, an additional field Authentication Type will be displayed in the Manager with the following choices: Local, LDAP, RADIUS:PAP, and RADIUS:CHAP.

:

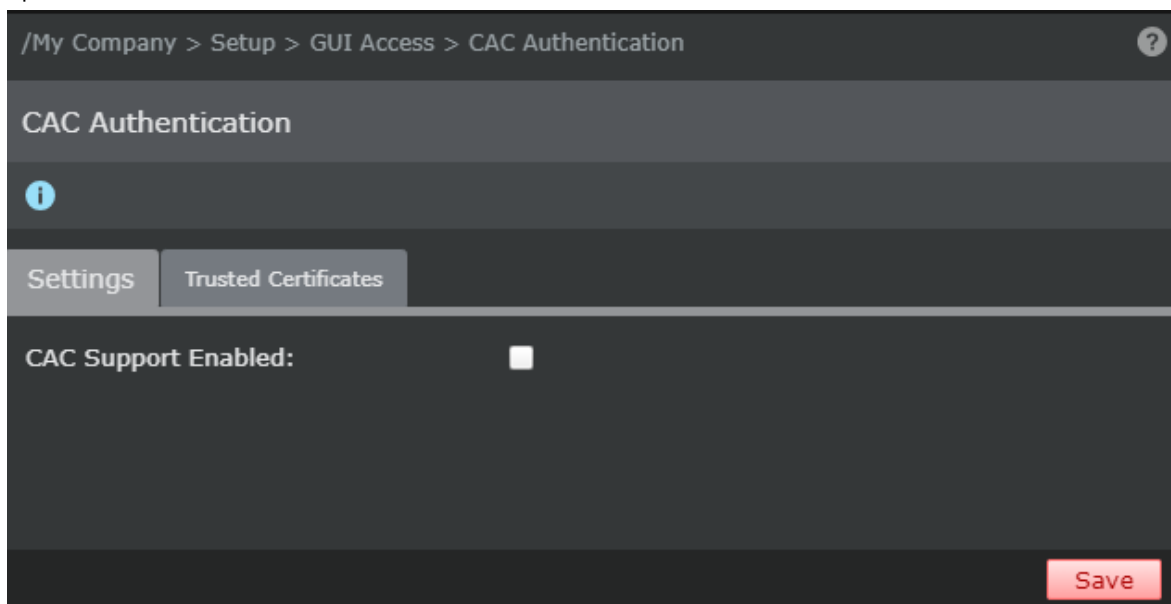
## Enable the CAC authentication

The CAC authentication feature is disabled by default. It is mandatory to set up the CAC user accounts and import the CAC certificates to the Manager, before enabling it.

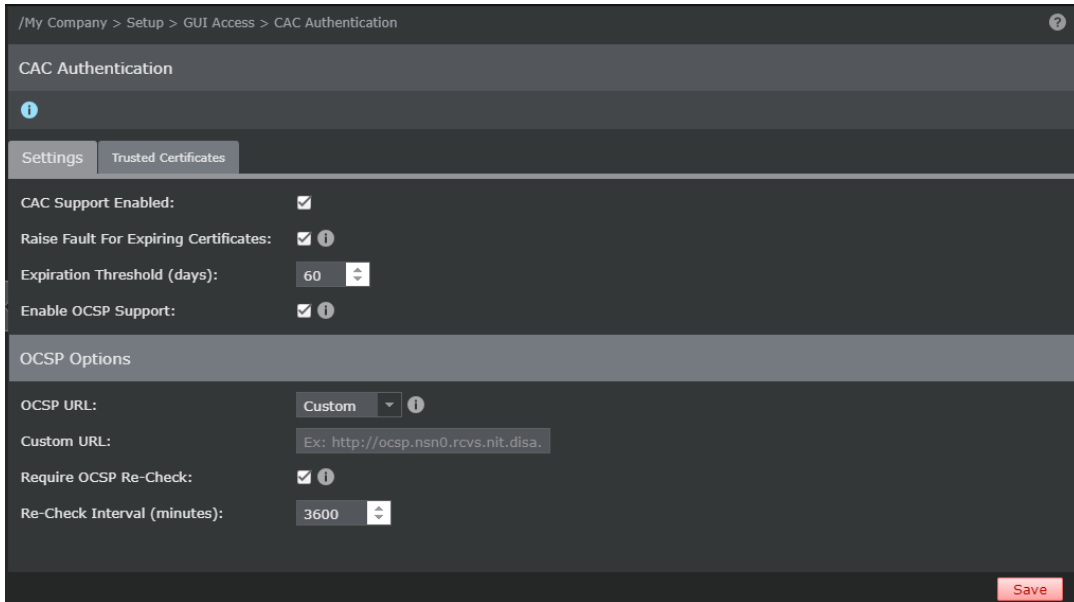
To enable CAC, do the following:

### Steps:

1. Log in to the Manager GUI.
2. Go to, Manager → <Admin Domain Name> → Setup → GUI Access → CAC Authentication. The CAC Authentication page opens.






3. In the Settings tab, configure the CAC Authentication as needed.



The table below describes the fields available for configuration:

Field	Description
CAC Support Enabled	Select the checkbox to enable CAC Authentication. By default, the CAC Authentication is disabled.
Raise Fault for Expiring Certificates	Select the checkbox to configure the Manager to generate faults when a trusted certificate is about to expire.
Expiration Threshold (days)	<p>Number of days for the trusted certificate expiration when a fault is generated in the Manager.</p> <p><b>Note:</b> The Expiration Threshold (days) can be within the range of 30 to 60 days only.</p> <p><b>Note:</b> The Expiration Threshold (days) can be configured only when the Raise Fault for Expiring Certificate option is enabled.</p>

Field	Description
Enable OCSP Support	Select the checkbox to enable OCSP Support. By default, the OCSP Support is disabled.
<b>OCSP Options</b>	
OCSP URL	Select Default to use the OCSP URL defined in the trusted certificate or Custom to configure a unified OCSP URL for all trusted certificates in the Manager.
Custom URL	Specify the OCSP URL for authenticating the trusted certificates.   <b>Note:</b> The Custom URL field is available only when you have the OCSP URL option set to Custom.
Require OCSP Re-Check	Select Yes to verify the authenticity of the trusted certificate after a definite interval.
Re-Check Interval (minutes)	Specify the duration in minutes after which the authenticity of the trusted certificate is rechecked.   <b>Note:</b> The Re-Check Interval (minutes) can be within the range of 30 to 1440 minutes only.   <b>Note:</b> The Re-Check Interval (minutes) can be configured only when the Require OCSP Re-Check option is enabled.

4. Click Save.
5. Log in to the Manager shell.
6. Stop the Manager service using the **manager stop** command.

7. Restart the Manager service using the `manager start` command.

:

### Log on to the Manager using the CAC/PIV authentication

#### Steps:

1. Insert a card into the card reader.
2. Start a fresh browser session for the Manager. You are prompted to choose the CAC/PIV certificate.
3. Select the certificate. You are prompted to enter the PIN.
4. Enter the PIN. A maximum of 3 attempts is allowed while entering PIN, following which, the user will be locked out. It is impossible to unlock a CAC/PIV card that is locked and the card has to be replaced. If the user name, certificate, and PIN match, you are directly given access to the Manager Home Page.

:

### Troubleshooting tips

- If the card is not inserted in the card reader, the Manager will not be accessible in this setup.
- When authenticating users through CAC, you do not have to enter your Manager user name and password while logging on.
- If you have imported a CA certificate to the Trusted Certificates in the Manager, you can't reimport the same certificate to the Manager.
- You are loading a CA certificate to the Manager, and yet you are unable to import it, then verify the validity of the certificate and make sure it is not expired.
- You have imported the relevant CA into the Manager, and yet you are unable to view the Manager Login page, then check whether a firewall is blocking your access to destination port 443 on the Manager server.
- If you are able to view the Manager Login page but are unable to log onto the Manager, it means that the user name on the CAC card does not match the user name in the Manager database. To remedy the problem, verify that the user name on the CAC card exactly matches the Manager user name.

:

### 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:

#### Steps:

1. Close all client connections. See [Closing all client connections](#).

2. Stop the Trellix IPS Manager service.
3. Stop the Trellix IPS Manager Watchdog service.
4. Stop the Trellix IPS Manager database service.

:

### Shut down the Central Manager

1. Close all client connections.
2. Stop the Trellix IPS Central Manager service.
3. Stop the Trellix IPS Manager Watchdog service.
4. Stop the Trellix IPS Manager database service.

#### Note

In the event of a crash, 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.

#### Steps:

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 the Manager Home page and log out of all open browser sessions.

:

### Shut down using the Trellix IPS Manager system tray icon in the Windows based Manager

#### Steps:

1. Right-click the Manager/Central Manager icon in your System Tray. The Trellix icon is displayed.

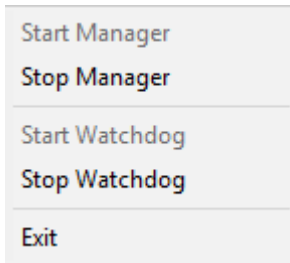
---

Trellix IPS Manager Service



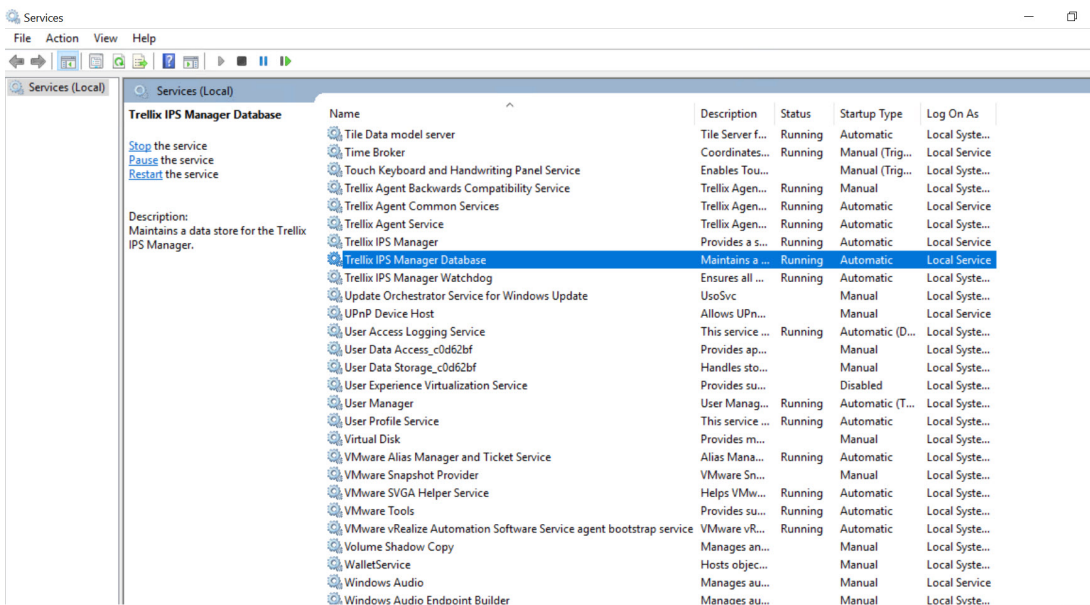
2. Select Stop Manager or Stop Central Manager. Once this service is completely stopped, continue to the next step.

## Stop Central Manager Service option



3. Go to Start → Settings → Control Panel.
4. Open Administrative Tools.
5. Open Services.
6. Find and select Trellix IPS Manager Database or Trellix IPS 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.

## Stop Service option



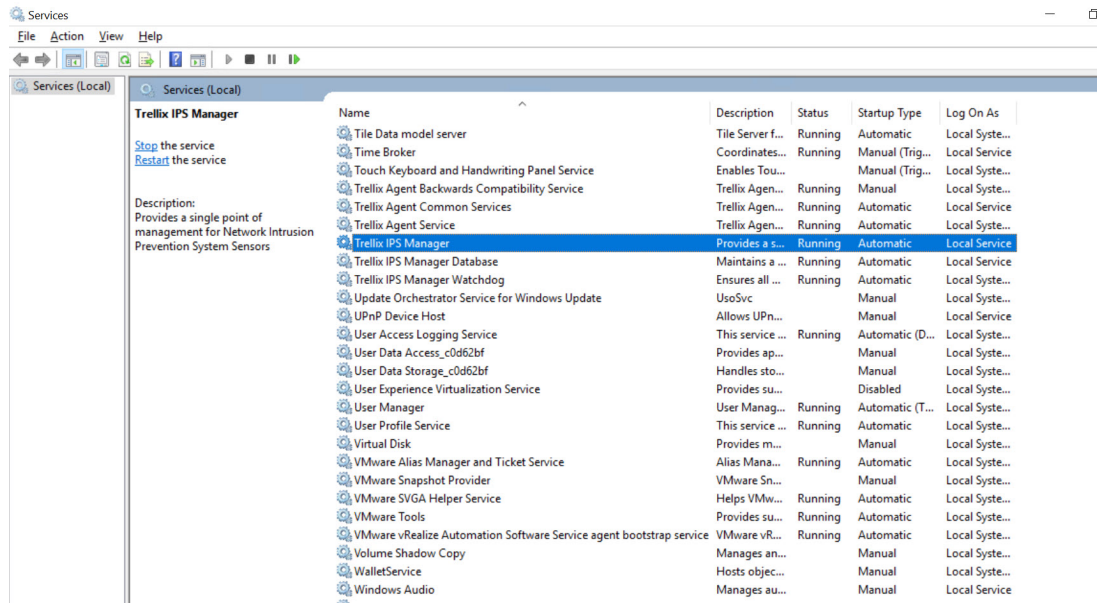
8. You can now safely shut down/reboot your server.

## Shut down using the Control Panel in the Windows based Manager

Steps:

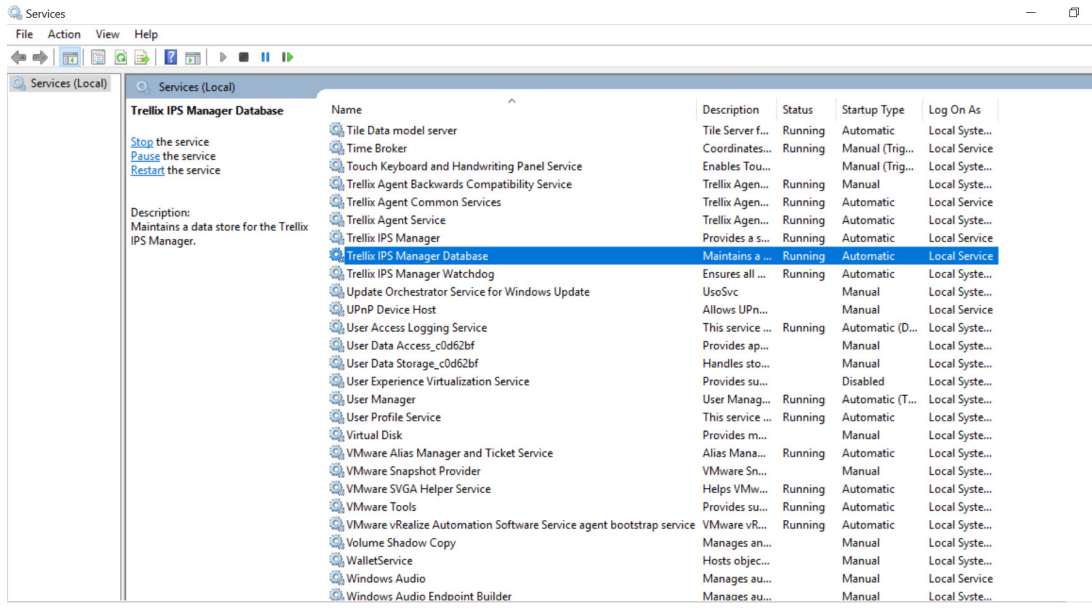
1. Go to Start → Settings → Control Panel.
2. Open Administrative Tools.
3. Open Services.
4. Select Trellix IPS Manager Service or Trellix IPS Central Manager Service in the services list under the Name column.
5. Click the Stop Service button. Once this service is completely stopped, continue to the next step.

Stop Service option



6. Find and select Trellix IPS Manager Database or Trellix IPS 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.

Service window



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

## Shutdown using the Manager shell in the Linux based Manager

### Steps:

1. Log in to the Manager shell.
2. Stop the Trellix IPS Manager Service or Trellix IPS Central Manager Service using the **manager stop** command.
3. Stop the Trellix IPS Manager Database service or Trellix IPS Central Manager Database service using the **database stop** command.
4. You can now safely shut down/reboot your Linux based Manager server using the **shutdown/reboot** command respectively.

## 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 *Trellix Intrusion Prevention System Product Guide*.

### Note

For information on adding and deploying a Virtual IPS Sensor, see the section *Virtual IPS Sensor deployment* in *Trellix Virtual Intrusion Prevention System Product Guide*.



:

### Before you install Sensors

This section describes best practices for deployment of Trellix IPS Sensors 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 Trellix IPS requires basic knowledge of your network to help determine the level of configuration and amount of installed Sensors and 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.

#### Caution

Read the installation instructions before you connect the system to its power source.

#### Caution

To remove all power from the Sensor, unplug all power cords, including the redundant power cord.

#### Caution

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

### Caution

The Sensor has no ON/OFF switch. Plug the Sensor into a power supply ONLY after you have completed rack installation.

### Caution

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.

### Caution

This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.

### Caution

Do not remove the outer shell of the Sensor. Doing so will invalidate your warranty.

### Caution

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.

### Caution

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.

### Caution

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 users will be required to correct the interference at their 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.

#### Caution

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

:

### Unpack the Sensor

To unpack the Sensor:

#### Steps:

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](#).
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.

:

### Contents of the Sensor box

The following accessories are shipped in the Sensor box:

- One Sensor
- One power cord. Trellix 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
- One printed *Trellix Intrusion Prevention System Quick Start Guide*
- Release notes

:

### Cable specifications

This section lists the specifications for all cables to use with the IPS Sensor.

:

### Console port pin-outs

Trellix 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.

Pin #	Signal	Direction on Sensor
1	DCD	Output
2	RXD	Output
3	TXD	Input
4	DTR	Input
5	GND	not applicable
6	DSR	Output
7	RTS	Input

Pin #	Signal	Direction on Sensor
8	CTS	Output
9	No Connection	Not applicable

:

### Auxiliary port pin-outs

The Auxiliary (Aux) port is pinned as DTE using DB9 or RJ-45 connector so that it can be connected to a modem with a straight-through cable.

Pin #	Signal	Direction on Sensor
1	DCD	Input
2	RXD	Input
3	TXD	Output
4	DTR	Output
5	GND	n/a
6	DSR	Input
7	RTS	Output
8	CTS	Input
9	RI	Input

#### Note

The Auxiliary port is available only in NS9x00 and NS7x00 Sensor models.

:

## Management port pin-outs

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

Pin #	Signal	Direction on Sensor
1	TxD+	Output
2	TxD-	Output
3	RxD+	Input
4	These pins are terminated to ground through a 75 ohm resistor & capacitor.	
5		
6	RxD-	Input
7	These pins are terminated to ground through a 75 ohm resistor & capacitor.	
8		

### Note

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.

### Note

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.

Pin #	Signal	Direction on Sensor
1	TxD+	Output
2	TxD-	Output
3	RxD+	Input
4	These pins are terminated to ground through a 75 ohm resistor & capacitor.	
5		
6	RxD-	Input
7	These pins are terminated to ground through a 75 ohm resistor & capacitor.	
8		

:

## How to monitor port pin-outs

The following ports are relevant to monitoring port pin-outs:

- Gigabit Ethernet (GE) ports

:

### 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.

:

### Configuration of a Sensor

This section describes how to configure a Sensor. This information is generic to all Sensor appliance models.

### Note

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 *CLI commands* section in the *Trellix Intrusion Prevention System Product Guide*.

:

## Configuration overview

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

### Steps:

1. (Pre-installation) Establish a Sensor naming scheme for your Sensor.
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 Trellix IPS Manager Configuration page.
4. Configure the Sensor with a unique name and shared key value.
5. Configure 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](#) for more details.
7. Verify connectivity between the Manager and the Sensor. See [Verifying successful configuration](#) for more details.

:

## 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. Trellix recommends that you establish an easily recognizable naming scheme prior to deployment, which indicates your Sensors' locations or purposes, and ensures unique names. The Manager will not recognize two Sensors with identical names.

Sensors are represented by name in several areas of Trellix Intrusion Prevention System and its alert data: the Manager Configuration page, alert and configuration reports, and the Attack Log. So, 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.

### Note

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 them. Later, configuration information is pushed from Manager to Sensor. The Manager does not poll the network to discover the Sensor.

### Note

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 Device Manager page.

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

### Note

The process of installing and connecting a Sensor is described in the *Trellix Intrusion Prevention System Product Guide* for each Sensor model.

The following steps describe how to add a Sensor to the Manager:

1. Start the Manager software.
2. Log on to the Manager. The default username is **admin**; the default password is **admin123**.

### Note

Trellix strongly recommends that you change the default password for security purposes. The new password must be at least 8 characters in length and must contain a combination of numbers, characters, and special characters. For more information on the password control, see section *Configure password complexity settings* in *Trellix Intrusion Prevention System Product Guide*.

3. Go to Devices → <Admin Domain Name> → Global → Device Manager.  
The Device Manager page is displayed.

4. Select the Sensors tab and click . The Add Device - Step 1 of 2 panel is displayed.

---

Add Device - Step 1 of 2 panel

The screenshot shows a dark-themed dialog box titled "Add Device - Step 1 of 2". It contains the following fields and controls:

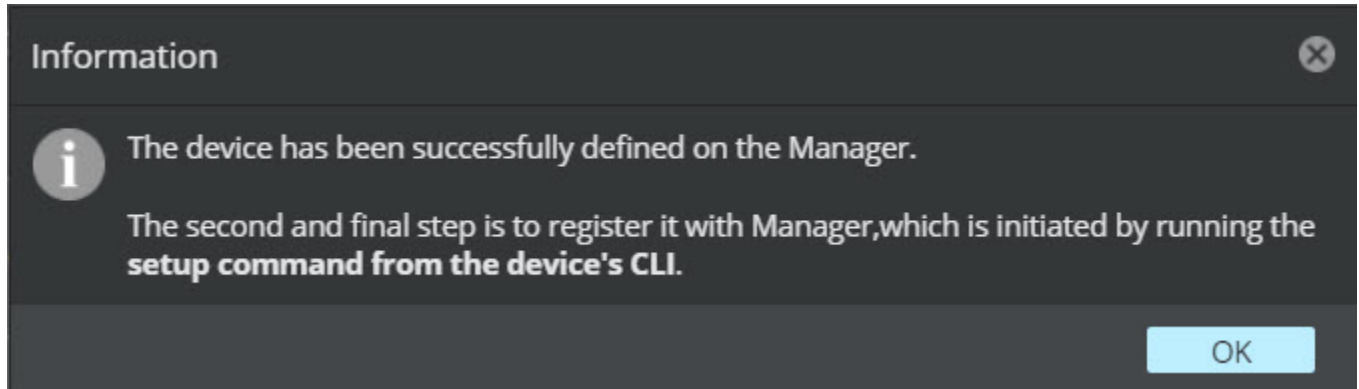
- Owner Domain: /My Company
- Name: 1-25 characters (with an information icon)
- Shared Secret: 8-25 characters (with an information icon)
- Confirm Shared Secret: 8-25 characters
- Device Type: (dropdown menu with an information icon)
- Deployment Mode: (dropdown menu with an information icon)
- Contact Information: (text input field)
- Location: (text input field)
- Comment: Maximum 255 characters (text input field)
- Save button at the bottom right.

5. Type the same Device Name as you entered on the Sensor.

### Caution

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 the Sensor trying to communicate with the Manager.

6. Enter the Shared Secret. 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: ~ ` ! @ # \$ % ^ & \* ( ) \_ + - = [ ] { } \ | ; : " ' , . < ? /
7. Enter the Confirm Shared Secret.
8. Ensure the selected Device type as IPS Sensor.
9. Select the Deployment Mode as Direct or Indirect from the drop-down.
10. (Optional) Type the Contact Information.
11. (Optional) Type the Location.
12. (Optional) Type the Comment.
13. Click Save to add the device to the Manager.  
An Information dialog box is displayed to confirm the addition of Sensor. Click OK.



:

## 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 *CLI commands* section in the *Trellix Intrusion Prevention System Product Guide*.

### Note

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 *CLI commands* section in the *Trellix Intrusion Prevention System Product Guide* for specific details on the usage of command.

### Steps:

1. Open a hyperterminal session to configure the Sensor. (For instructions on connecting to the Console port, see the section *Connect the cable to the Console port*, in the *Trellix Intrusion Prevention System NS-series 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**.

### Note

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

### Note

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 *Trellix Intrusion Prevention System NS-series Sensor Product 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**

### Note

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 section *Conditions requiring a Sensor reboot* in *Trellix Intrusion Prevention System Product 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: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 sensor gateway-ipv6 2001:0db8:8a2e::0111**

### Note

The following are the default set of values for the management port:

IP Address : 192.168.100.100

Netmask : 255.255.255.0

Gateway : 0.0.0.0

This allows you an additional option of configuring the Sensor via the management port apart from the console port.

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: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 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 *Trellix Intrusion Prevention System Product 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.

### Note

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`

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. A password must be between 8 and 25 characters, is case-sensitive, and can consist of any alphanumeric character or symbol.

### Note

Trellix 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.

10. 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 *CLI commands* section in the *Trellix Intrusion Prevention System Product Guide*.)

- In the Manager Dashboard, check the System Faults status. (See if the Sensor is active. If the link is yellow, click on the cell to see the System Faults on the Sensor.)
- In the Manager, go to Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Physical 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.

### Note

If you have difficulty in troubleshooting the processes described above, refer to *Trellix Intrusion Prevention System Product Guide*. See *Trellix Intrusion Prevention System Product 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

### Note

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

:

## Change the Sensor IP or the Manager IP

Steps:

1. **Change the Manager IP**
  - a. Log in to the Sensor CLI.
  - b. Execute the `deinstall` command to remove trust between the Manager and the Sensor.
  - c. Execute the `set manager ip <IP_address_of_the_Manager>` command to change the IP address of the Manager in the Sensor.

- d. Execute the **set sensor sharedsecretkey** command to establish trust between the Manager and the Sensor. 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.

### Note

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**.

## 2. Change the Sensor IP

- a. Open a hyperterminal session to change the IP address of the Sensor. (For instructions on connecting to the Console port, see the section *Cabling the Console Port*, in *Trellix Intrusion Prevention System NS-series Sensor Product Guide* for your Sensor model.)
- b. Execute the **set sensor ip <IP\_address\_to\_be\_assigned\_to\_the\_Sensor>** to assign an IP address to the Sensor.

### Note

Make sure the subnet mask and gateway addresses are configured correctly.

### Note

The trust between the Manager and the Sensor is removed when the IP address of the Sensor is changed. You must re-establish the Manager trust to continue the Manager-Sensor communication.

- c. Reboot the Sensor by executing the **reboot** command.

:

## 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 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.

:

### Add and configure Sensors

The process of adding and configuring a Sensor adding a Sensor to the Manager and Configure the Sensor using CLI.

:

### Add a Sensor to the Manager

To add a Sensor, perform the following steps:

Steps:

1. Go to Devices → `<Admin Domain Name>` → Global → Device Manager.  
The Device Manager page is displayed.



2. Select the Sensors tab and click .

The Add Device - Step 1 of 2 panel is displayed.

3. Enter relevant details in the Add Device - Step 1 of 2 panel.
  - a. Enter the Name of the device. The Sensor name must begin with a letter. The maximum length of the name is 25 characters.
  - b. Enter the Shared Secret. 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 lowercase (a,b,c,...z and A, B, C,...Z)
    - 10 digits: 0 1 2 3 4 5 6 7 8 9
    - 32 symbols: ~ ` ! @ # \$ % ^ & \* ( ) \_ + - = [ ] { } \ | ; : " ' , . < ? /

### Note

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.

- c. Enter the Confirm Shared Secret.
  - d. Select the required Device Type as IPS Sensor or NTBA Appliance.
4. Select the Deployment Mode as either Direct or Indirect from the drop-down. In Direct mode, pending changes are delivered directly from the Manager to Sensor. It is the recommended mode. In Indirect mode, when trust is established between the Manager and the Sensor, the initial configuration update from Manager to Sensor will be stopped. You can toggle between Direct and Indirect modes in the Manager by navigating to Devices → <Admin Domain Name> → Devices → <Device Name> → Summary. In the Sync monitor, select Direct or Indirect against Sync Mode and click Save. The Sensor status will be shown as **good** in the CLI only after successful configuration update by enabling the Direct mode.
  5. If required, enter the Contact Information, Location, and Comment details.
  6. Click Save.

An Information dialog box is displayed to confirm the addition of Sensor. Click OK.

The new Sensor is displayed in the Sensors tab of Device Manager page.

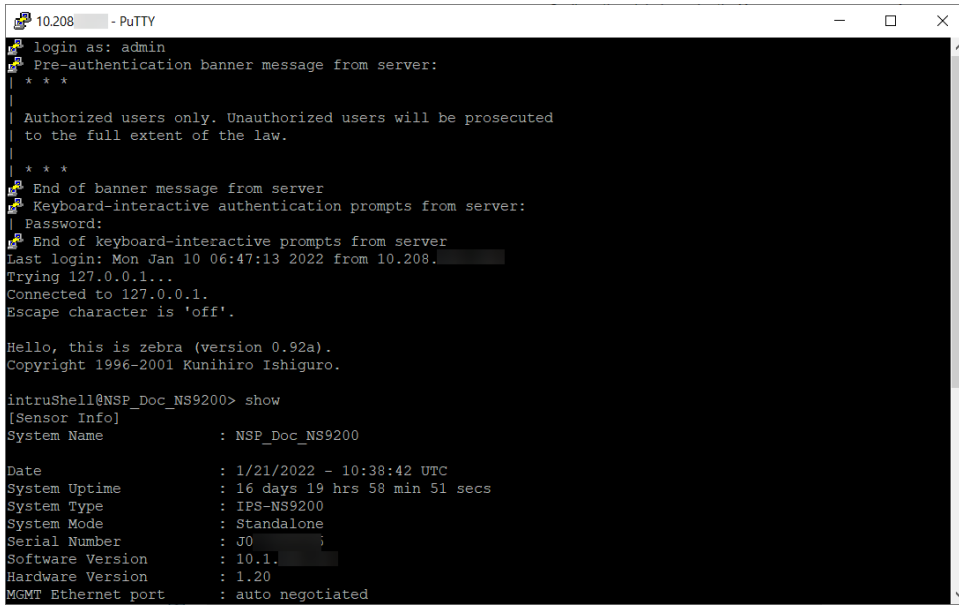
## Configure the Sensor using CLI

### Steps:

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

---

CLI window



```
10.208 - PuTTY
login as: admin
Pre-authentication banner message from server:
| * * *
|
| Authorized users only. Unauthorized users will be prosecuted
| to the full extent of the law.
|
| * * *
|
| End of banner message from server
Keyboard-interactive authentication prompts from server:
| Password:
|
| End of keyboard-interactive prompts from server
Last login: Mon Jan 10 06:47:13 2022 from 10.208.
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is 'off'.

Hello, this is zebra (version 0.92a).
Copyright 1996-2001 Kunihiro Ishiguro.

intruShell@NSP_Doc_NS9200> show
[Sensor Info]
System Name      : NSP_Doc_NS9200
Date             : 1/21/2022 - 10:38:42 UTC
System Uptime    : 16 days 19 hrs 58 min 51 secs
System Type      : IPS-NS9200
System Mode      : Standalone
Serial Number    : J0
Software Version : 10.1.
Hardware Version : 1.20
MGMT Ethernet port : auto negotiated
```

For instructions, see the section *Connect the cable to the Console port* in *Trellix Intrusion Prevention System NS-series 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**

### Note


Trellix 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**

### Note

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**

 Note

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 *Trellix Intrusion Prevention System Product 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 *Trellix Intrusion Prevention System Product 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.

 Note

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 upto 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: ~ ` ! @ # \$ % ^ & \* ( ) \_ + - = [ ] { } \ | ; : " ' , . < /

 Caution

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

10. To exit the session, type **exit**

:

## Managing licenses for NS9500, NS7500, and NS3500 Sensors


The NS9500, NS7500, and NS3500 Sensors require a software license to activate the baseline throughput of 10 Gbps on NS9500 Sensors, 3 Gbps on NS7500, and 750 Mbps on NS3500 Sensors.

The license is provided as a .zip or .jar file (for example, CapacityLicense3Gig.jar for a new license and CapacityLicense3to5.jar for an upgrade license). The Manager supports both the formats. The license procured contains the details of the Sensor's throughput. The Manager checks the compliance periodically to check the number of licenses against the Sensor's throughput.

 **Note**

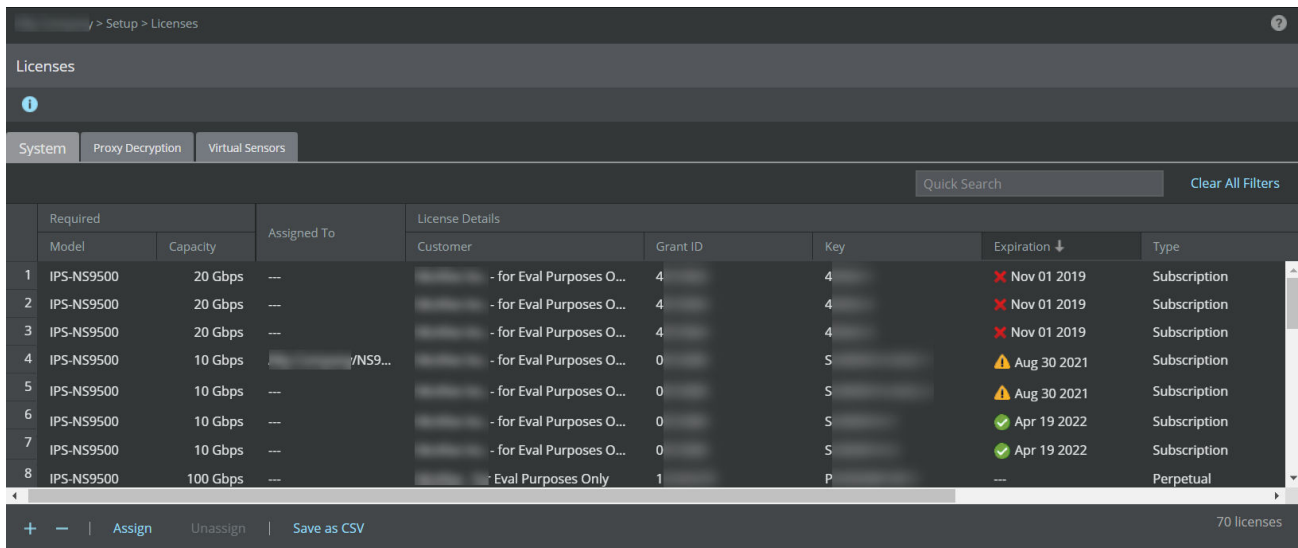
You must first purchase a license to enable traffic inspection in NS9500, NS7500, and NS3500 Sensors. To obtain a license, contact Trellix Sales.

In case of the NS9500 standalone and stack, and NS7500 Sensors, an additional license or upgrade license is required to increase the throughput of the Sensor. Various throughputs available are as follows:

Sensor	Existing license	Additional license	Upgrade license
NS9500 standalone   <b>Note:</b> You must have a stack Sensors setup to upgrade licenses from standalone to stack.	10 Gbps	<ul style="list-style-type: none"> <li>• 20 Gbps</li> <li>• 30 Gbps</li> </ul>	<ul style="list-style-type: none"> <li>• 10 to 20 Gbps</li> <li>• 10 to 30 Gbps</li> </ul> Standalone to stack: <ul style="list-style-type: none"> <li>• 10 to 40 Gbps</li> <li>• 10 to 60 Gbps</li> <li>• 10 to 100 Gbps</li> </ul>
	20 Gbps	30 Gbps	<ul style="list-style-type: none"> <li>• 20 to 30 Gbps</li> </ul> Standalone to stack: <ul style="list-style-type: none"> <li>• 20 to 40 Gbps</li> <li>• 20 to 60 Gbps</li> <li>• 20 to 100 Gbps</li> </ul>
	30 Gbps	NA	Standalone to stack: <ul style="list-style-type: none"> <li>• 30 to 40 Gbps</li> <li>• 30 to 60 Gbps</li> <li>• 30 to 100 Gbps</li> </ul>
NS9500 stack	40 Gbps	<ul style="list-style-type: none"> <li>• 60 Gbps</li> <li>• 100 Gbps</li> </ul>	<ul style="list-style-type: none"> <li>• 40 to 60 Gbps</li> <li>• 40 to 100 Gbps</li> </ul>






Sensor	Existing license	Additional license	Upgrade license
	60 Gbps	100 Gbps	60 to 100 Gbps
NS7500	3 Gbps	<ul style="list-style-type: none"> <li>• 5 Gbps</li> <li>• 7.5 Gbps</li> </ul>	<ul style="list-style-type: none"> <li>• 3 to 5 Gbps</li> <li>• 3 to 7.5 Gbps</li> </ul>
	5 Gbps	7.5 Gbps	5 to 7.5 Gbps

You can upload the license from the Licenses page in the Manager. In the Manager, select Manager → <Admin Domain Name> → Setup → Licenses.



The following details are displayed on the System tab:

Option	Definition
Required	Model – Sensor model compatible with the license Capacity – Throughput limit for the license
Assigned To	Name of the Sensor assigned to the license

Option	Definition
License Details	<p>Customer – Customer for whom the license file was generated</p> <p>Grant ID – Trellix Grant ID of the corresponding customer</p> <p>Key – License key number of the customer</p> <p>Expiration – Applicable only for demo and subscription licenses</p> <ul style="list-style-type: none"> <li>•  : Valid license</li> <li>•  : Expired license</li> <li>•  : Expired license running on grace period</li> </ul> <div style="background-color: #e1f5fe; padding: 10px; margin: 10px 0;"> <p> <b>Note:</b> A grace period of <b>30 days</b> is provided to subscription-based System licenses after they expire.</p> </div> <p>Post grace period, the Sensor continues to inspect traffic, and operates with the existing signature set and configuration. The Manager, however, will not be able to deploy new signature sets or policies to the Sensor until a valid license is assigned.</p> <p>Type – Displays if the license is Perpetual, Subscription, or Evaluation (Demo) type</p> <div style="background-color: #e1f5fe; padding: 10px; margin: 10px 0;"> <p> <b>Note:</b> It is recommended to install subscription license from Manager version 10.1.7.44 and later.</p> </div>
Added	<p>Time – Date in &lt;mm-dd-yy&gt; format, and time when the license was added</p> <p>By – Name of the user who added the license</p>
Comments	<p>Enables you to add your comment per license file that is imported. Double-click in the Comment field</p>

Option	Definition
	and enter your comment. Click outside this field and your comment is automatically saved.

The following actions can be performed on the System tab:

- [Add a license to the Manager](#)
- [Assign a license to a Sensor](#)
- [Unassign a license from a Sensor](#)
- [Upgrade an existing capacity license](#)
- [Remove a license from the Manager](#)


For more information about Proxy Decryption tab, refer [System and Proxy Decryption tab](#), and for assigning licenses to the Virtual Sensors, refer [Managing licenses for Virtual Sensors](#).

:

## Add license to the Manager

To upload the license, perform the following steps:

### Steps:

1. Go to Manager → <Admin Domain Name> → Setup → Licenses.
2. Click the System tab.
3. Click .  
The Add License pop-up window opens.
4. Click Browse. Navigate to the location where the license is saved. Select the license and click Open.

### Note

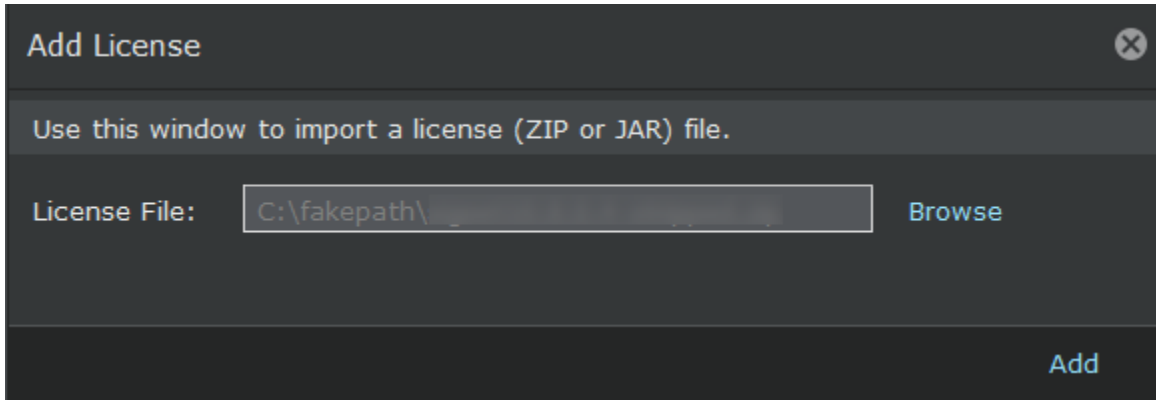
The supported license formats are .zip and .jar.

### Note

It is recommended to add subscription license from Manager version 10.1.7.44 and later.

---

Upload license to the Manager



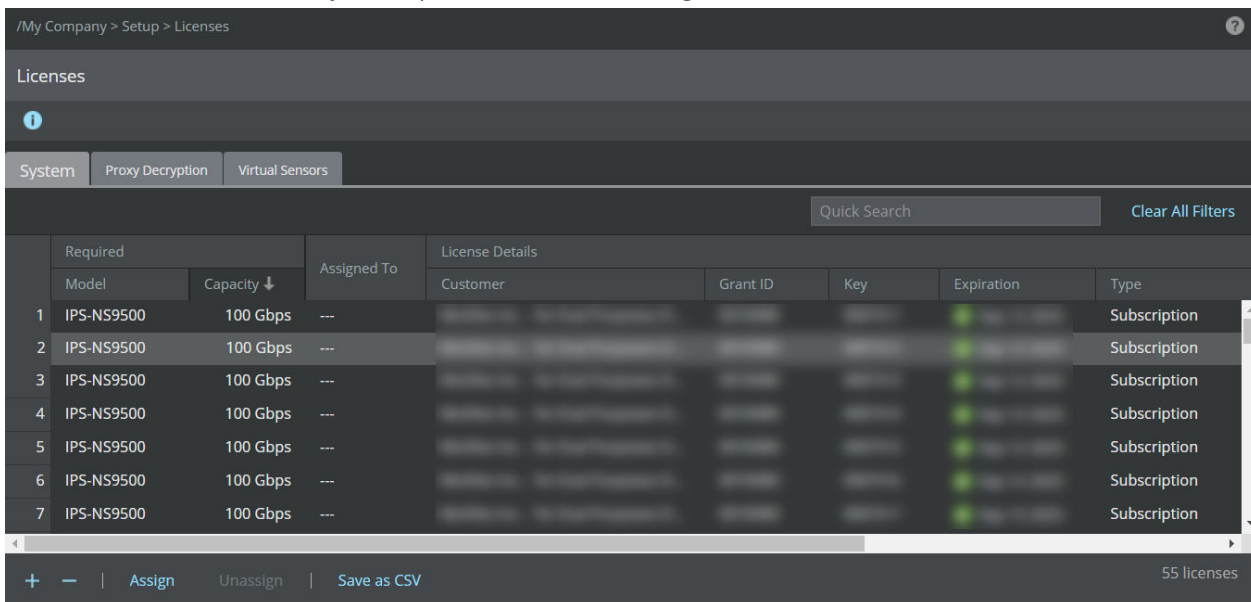
5. Click Add.  
The license is uploaded to the Manager.
6. (Optional) Click Save as CSV to export the license usage details as .csv file.

## Assign a license to a Sensor

To assign the license, perform the following steps:

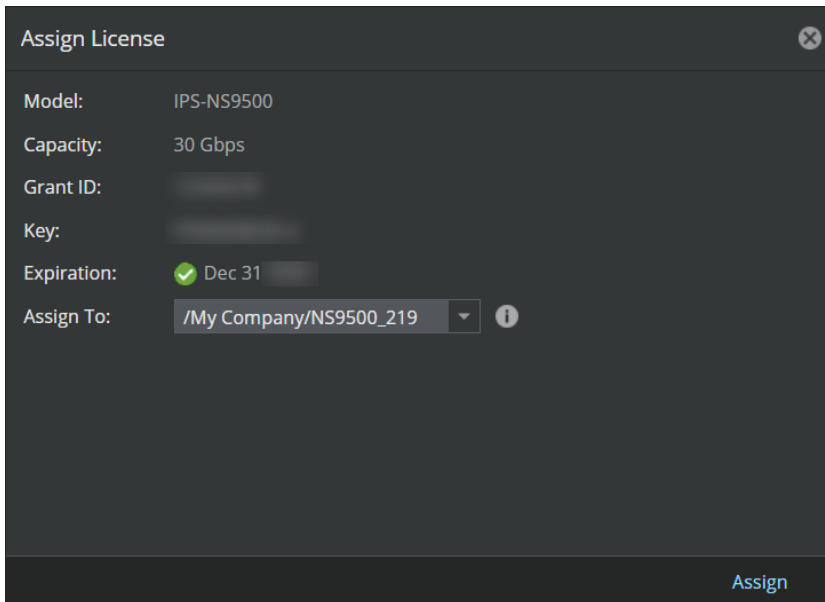
### Steps:

1. Navigate to Manager → <Admin Domain Name> → Setup → Licenses.
2. Click the System tab.
3. Choose the license that suits your requirement and click Assign.





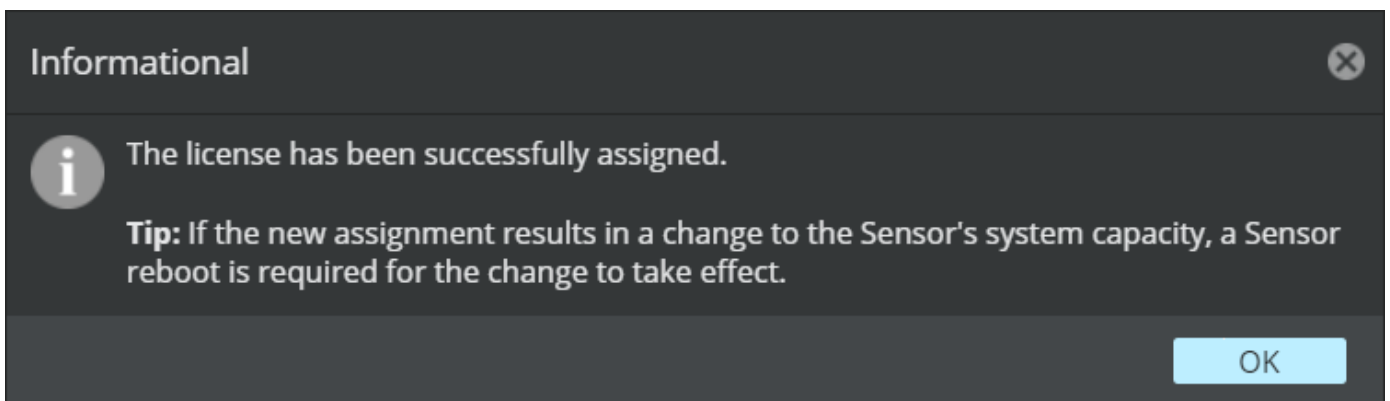
4. The Assign License pop-up window opens, click the Assign To drop-down menu and select the Sensor.
5. Click Assign to assign the license to the Sensor.



### Note

In case you are replacing an existing license, a Confirmation dialog-box opens. To confirm license replacement, click OK, else, click Cancel.

6. Upon successful license assignment, an **Informational** dialog-box opens stating the license has been successfully assigned. Click OK to close it.



### Note

In case you are replacing an existing license with a license of varied capacity, you must reboot the device for the new capacity to take effect. If you are replacing an existing license with a same capacity license, reboot is not required.

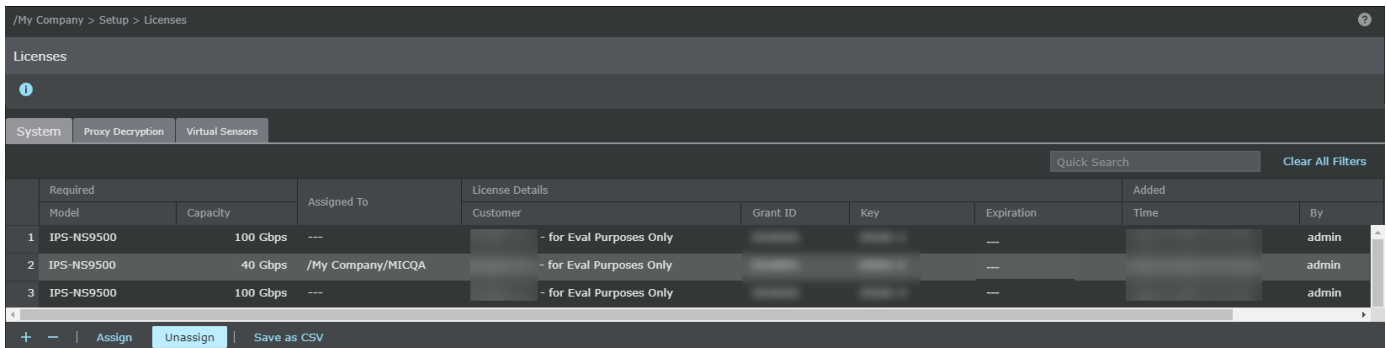
:

## Unassign a license from a Sensor

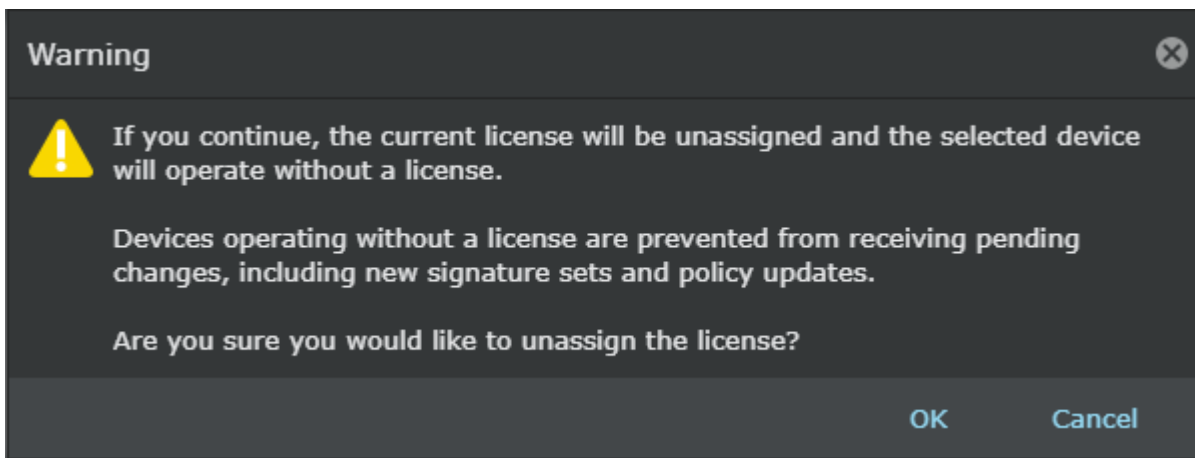
To unassign the license, perform the following steps:

### Steps:

1. Go to Manager → <Admin Domain Name> → Setup → Licenses.
2. Click the System tab.
3. Select the license you wish to unassign.



4. Click Unassign.
5. Click Ok.



Once a license is unassigned from a Sensor, the Manager will not be able to deploy pending changes, including new signature sets and policy updates to the Sensor.

:

## Upgrade an existing capacity license

Points for considerations:

Consider the following points before you upgrade the capacity license:

- This section is not applicable to Sensors running on subscription based licenses. It is applicable only for Sensors running with perpetual licenses.
- For HA pair, the Sensors in the HA will have to run with the same capacity for the deployment of updates to be successful.
- If you are upgrading your capacity license, you must reboot your Sensor for the change to take effect.
- If you select an existing license (from a zip file containing one license) and if the Sensor assignment is not done, the existing license is removed and replaced with the new capacity license.
- If you select an existing license (from a zip file containing two or more licenses) and if the Sensor assignment is not done, then only one of the existing license which is selected from the list of licenses available is removed and replaced with the new capacity license. For example, if there are two licenses with license keys L001-1 and L001-2 in a zip file, only one of it will be replaced with the new license with a change to the license key.
- If you select an existing license (from a zip file containing one license) and if the Sensor assignment is done, the existing license is removed and replaced with the new capacity license. This upgraded license is automatically assigned to the Sensor.

### Note

If the Sensor also has an existing SSL proxy decryption license assigned and its capacity is same as the old system license, then you must purchase an SSL proxy decryption license with the same capacity as the upgraded system license, to enable signature file push to the Sensor.

- If you do not have an existing license with x capacity, you cannot add an upgrade license with (x + y) capacity. For example, if you do not have a 10G license available in the Manager, you cannot add an upgrade license from 10G to 20G.....100G in the Manager.
- After the existing license (x) is replaced with a new license (x+y), you cannot re-import the old license (x) from which you upgraded.
- Demo licenses cannot be upgraded.
- An upgraded capacity license can be further upgraded.
- You can upgrade the existing capacity license as long as the license is not expired.
- You can upgrade the existing NS9500 standalone to new NS9500 stack, but you must reassign the license manually to the stack.
- If the bundled zip file contains upgrade license files and new license files, you are prevented from adding it to the Manager.

### Note

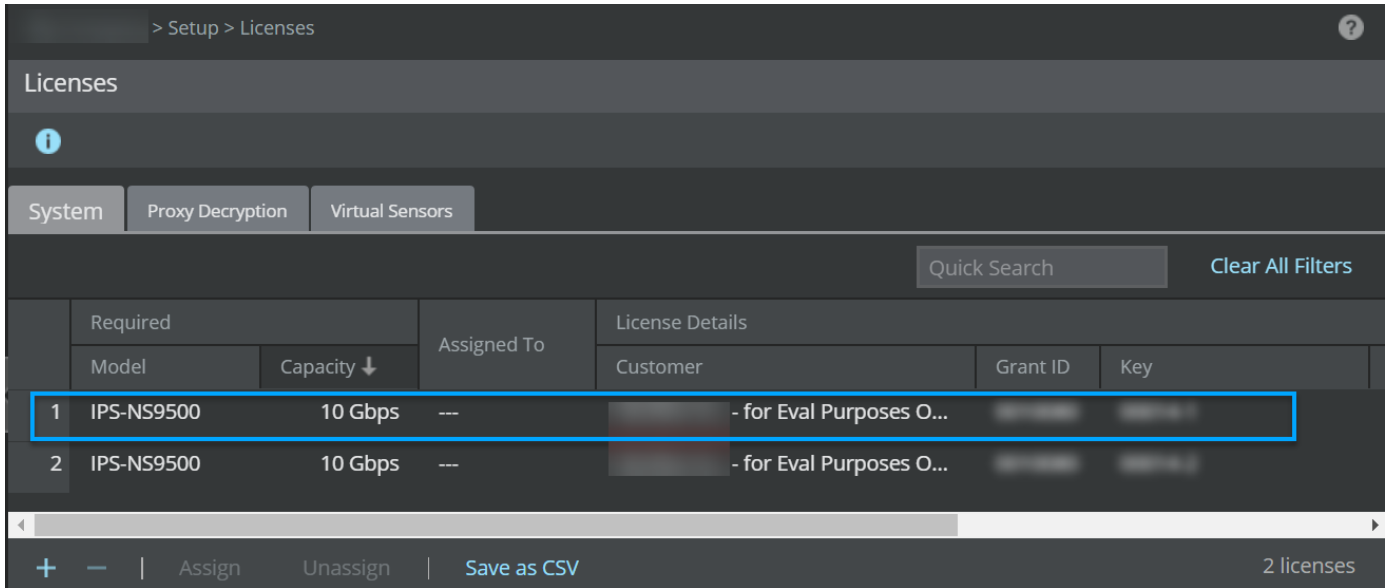
In such a case, unzip the file and add the licenses to the Manager individually.

### Steps:

To upgrade an existing capacity license, perform the following steps:

1. Go to Manager → <Admin Domain Name> → Setup → Licenses.

2. Click the System tab. The system tab with existing licenses:



3. Click .

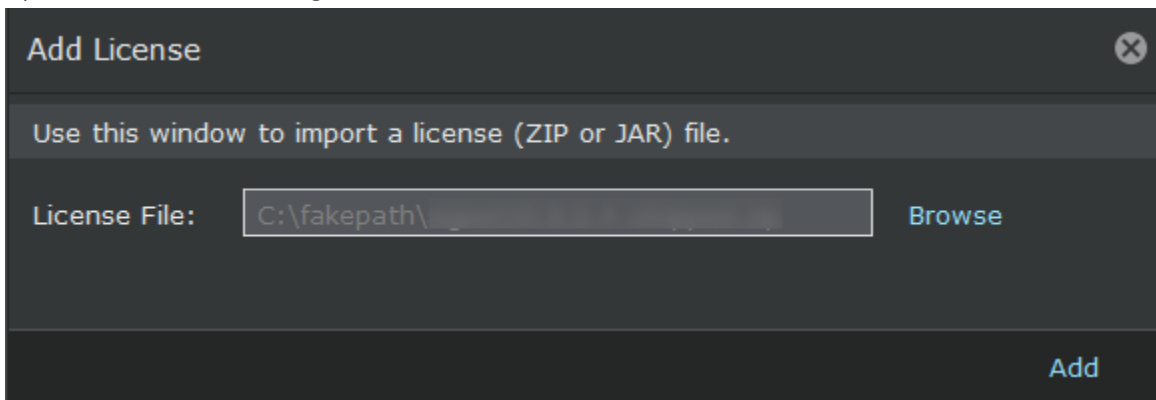
The Add License pop-up window opens.

4. Click Browse. Navigate to the location where the upgrade license is saved. Select the license and click Open.

### Note

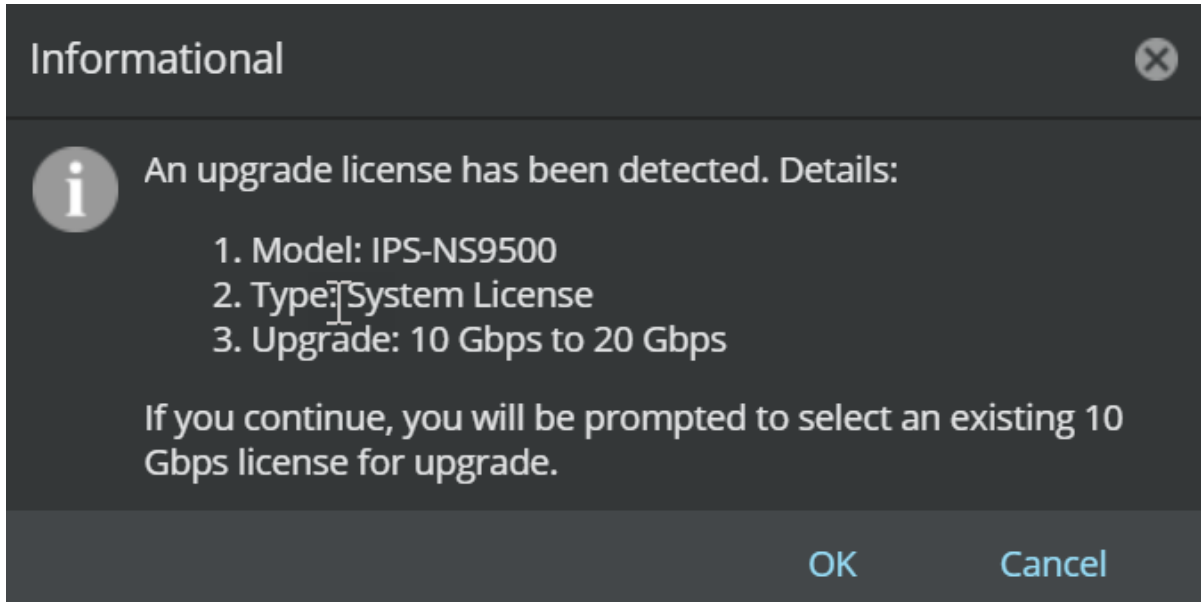
The supported license formats are zip and jar.

Upload license to the Manager

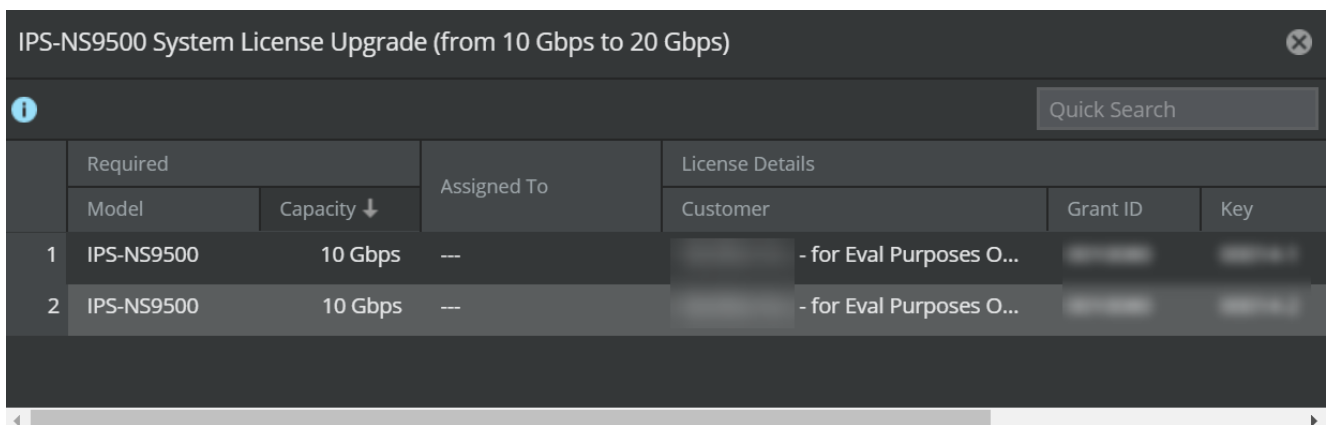


5. Click Add.

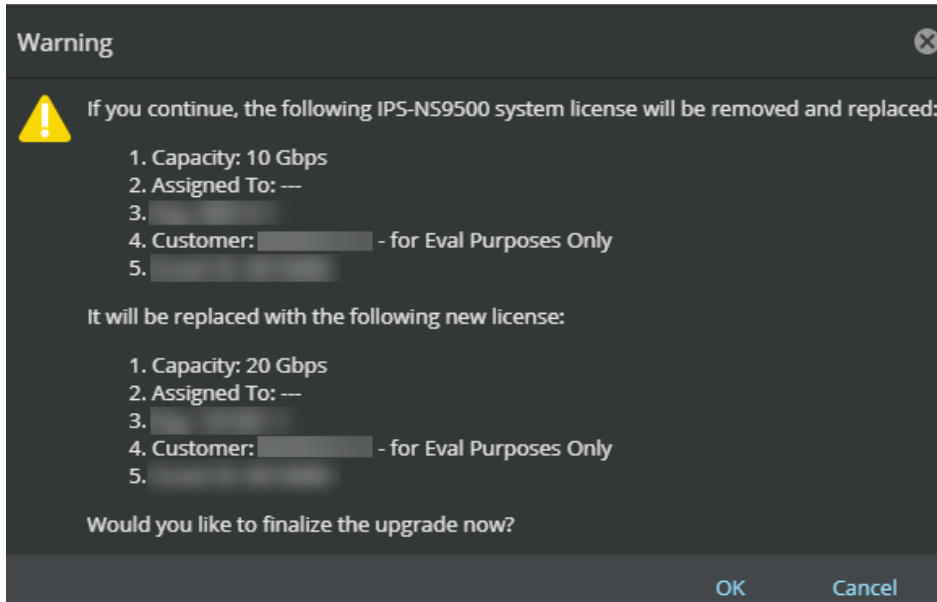
a. An informational message window appears. Click OK.



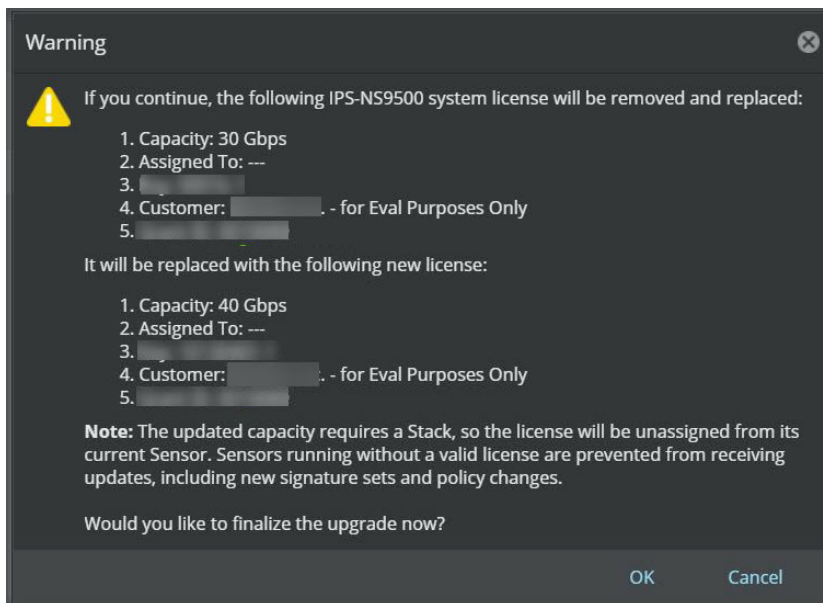
- b. <Sensor name> System license upgrade (from x Gbps to x+y Gbps) window appears which displays all the licenses present in the Manager for that particular capacity. Double click on the license you wish to upgrade the capacity license for.



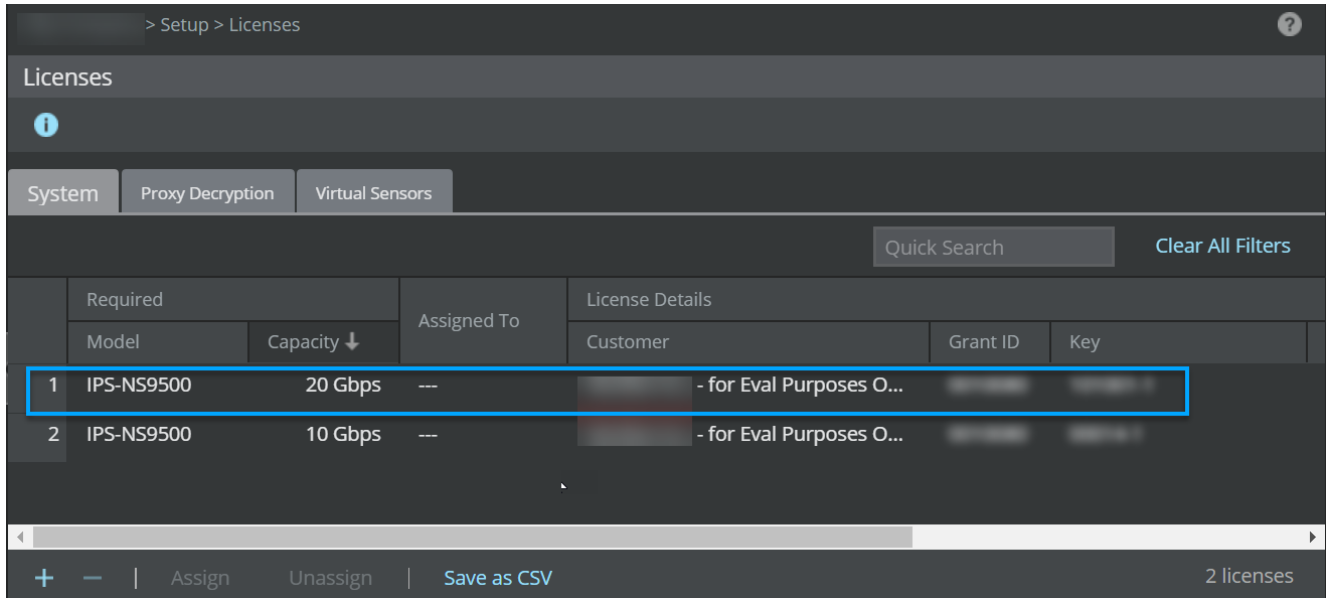
- c. A warning message that the existing system license will be removed and replaced with a new license appears. Click OK.



if you are upgrading from a standalone Sensor to a stack Sensor, the following warning message is displayed. Click OK.



The existing system capacity license is replaced with the new capacity license.




6. (Optional) Click Save as CSV to export the license usage details as .csv file.

:

## Remove a license from the Manager

To remove a license, perform the following steps:

### Steps:

1. Go to Manager → <Admin Domain Name> → Setup → Licenses.
2. Click the System tab.
3. Select the license you wish to remove.
4. Click .
5. Click Ok. Once a license is removed from the Manager, you will not be able to deploy pending changes, update new signature sets and policy update to the Sensor from which the license is unassigned automatically upon deletion of the license.

:

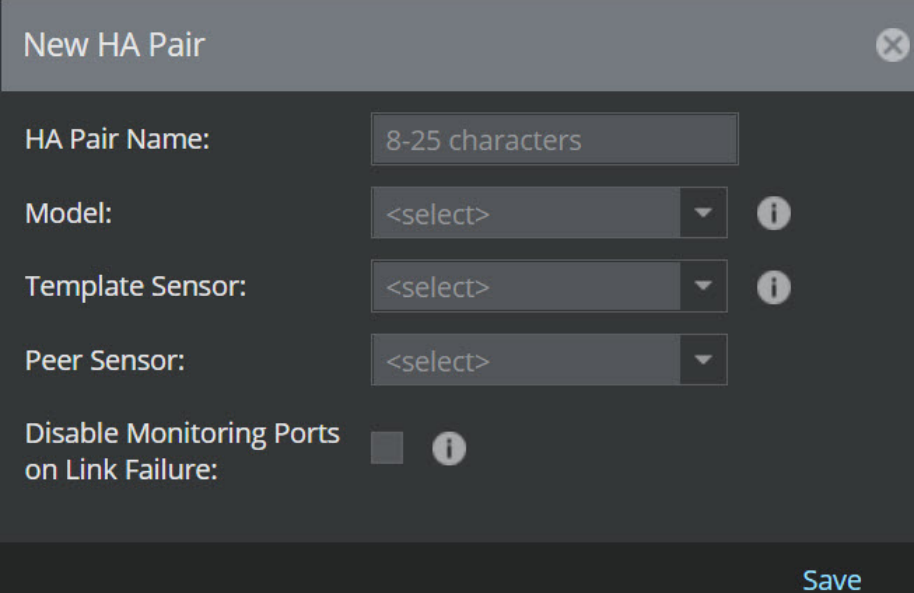
## Possible actions from the device list nodes

The following actions are possible through the Devices tab:

- **Managing Devices** — Add devices to the Manager; accept communication from 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 that apply to your Sensors are not pushed until you perform Devices → <Admin Domain Name> → Global → Device Manager, select the required Sensors from Sensors tab

and click Sync (applicable to all Sensors in a domain) or Devices → <Admin Domain Name> → Devices → <Device Name> → Deploy Pending Changes (single Sensor) action.

- **Updating software to all devices** — Download software and signature files from the Manager via Trellix IPS Update Server.
- **Creating HA Pairs** — Pair two devices for failover operation.



The screenshot shows a dark-themed dialog box titled "New HA Pair" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- HA Pair Name:** A text input field containing "8-25 characters".
- Model:** A dropdown menu with "<select>" and a downward arrow, accompanied by an information icon (i).
- Template Sensor:** A dropdown menu with "<select>" and a downward arrow, accompanied by an information icon (i).
- Peer Sensor:** A dropdown menu with "<select>" and a downward arrow.
- Disable Monitoring Ports on Link Failure:** A checkbox that is currently unchecked, accompanied by an information icon (i).

A "Save" button is located at the bottom right of the dialog box.

:

### Options available in the Devices page

The Devices page 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.

:

### Edit device settings

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

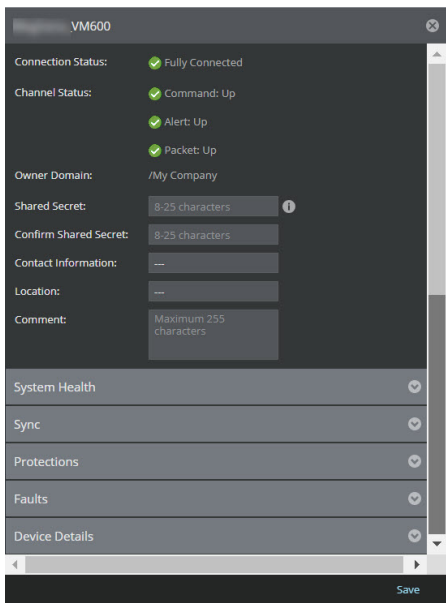


### Note

Trellix recommends to first change the Shared Secret from the Manager. 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:

1. Go to Devices → <Admin Domain Name> → Global → Device Manager.  
The Device Manager page is displayed.
2. Select the Sensors tab.
3. From the display list, double-click on the required Sensor  
Details panel with <Device Name> is displayed.



4. Make the required changes and click Save.

### Note

Double asterisks indicate that the data for the field is missing or that data has been retrieved from the database rather than from the device. This could indicate that the device is inactive or not initialized.

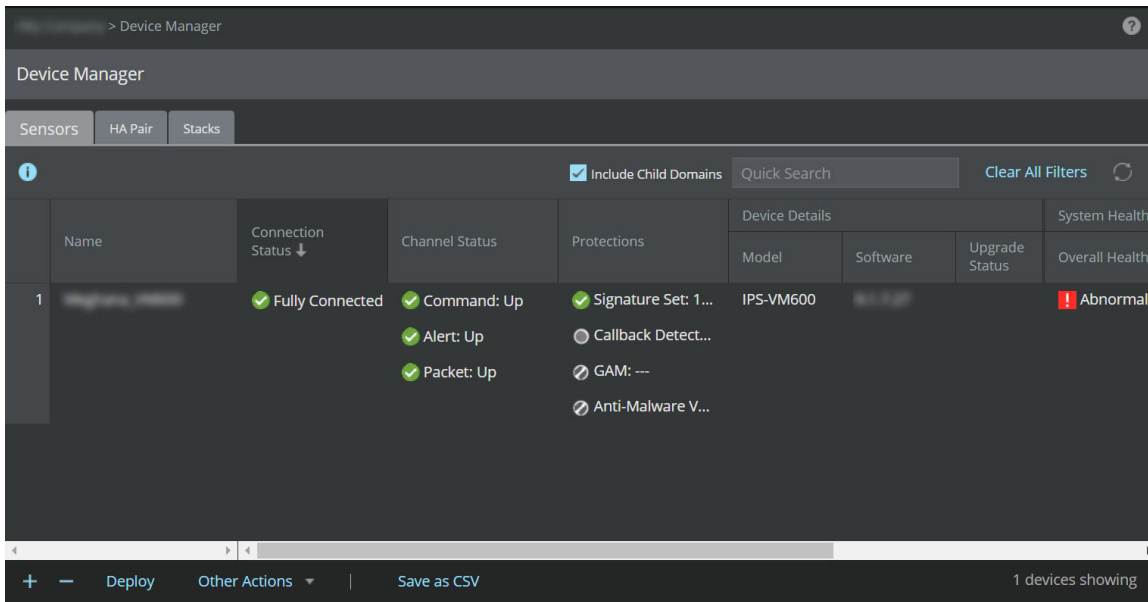
:


## Delete a device configuration

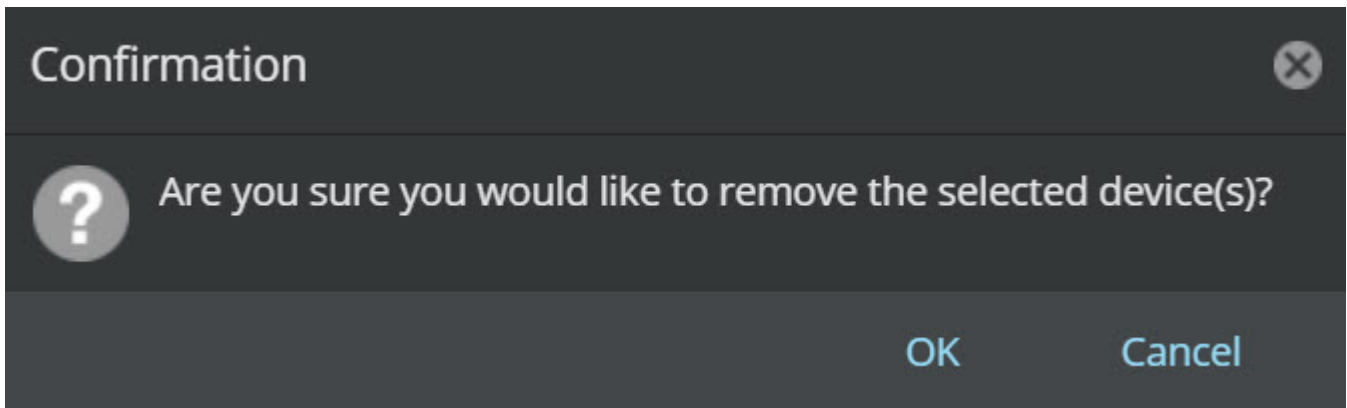
To delete a configured device in the Manager perform the following steps:

**Steps:**

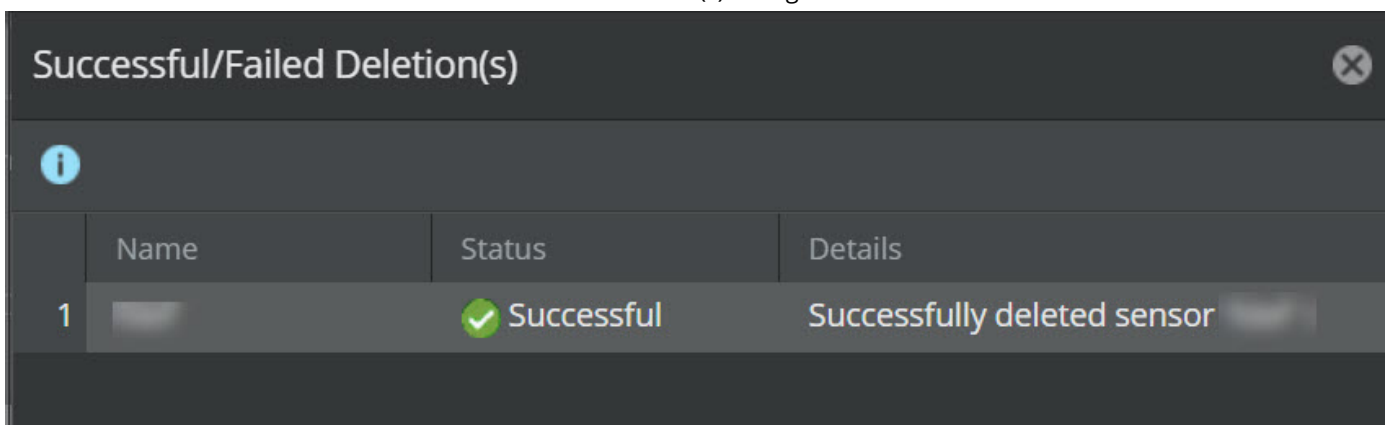
1. Go to Devices → <Admin Domain Name> → Global → Device Manager. The Device Manager page is displayed.



2. Select the Sensors tab.
3. Select the device(s) you wish to delete from the list. Then, click .
4. A **Confirmation** dialog box is displayed. Click OK to remove the selected device(s) from the Manager.



5. You can view the delete status from Successful/Failed Deletion(s) dialog box.



### 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 and then re-attempt the delete action.

:

### 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 Trellix, 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 several tabs of the Devices node.
- Policy changes are updated on the Sensor or NTBA Appliance in case of a newly applied policy, or change made to the current enforced policy.
- Signature updates contain new and/or modified signatures that can be applied to the latest attacks.
- When policy and rule updates are applied to the devices, the current traffic analysis is not impacted until the last phase of configuration updates (i.e the Manager status update is at 95%).

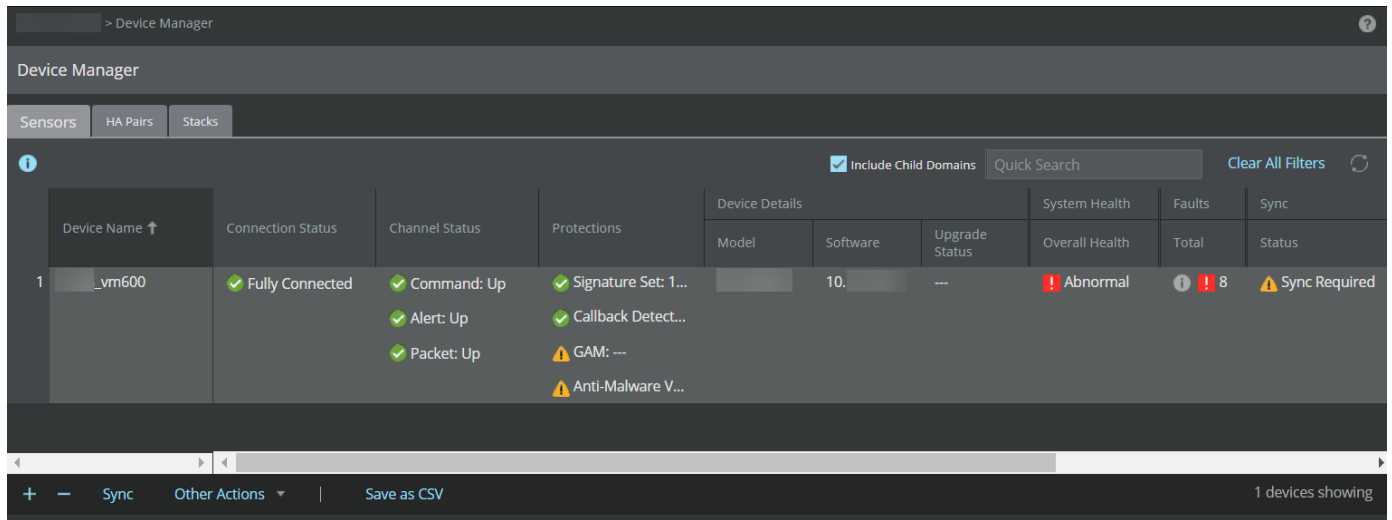
Refer the following steps to deploy the configuration changes to all devices in the admin domain or at a device level.

### Steps:

1. Go to Devices → <Admin Domain Name> → Global → Device Manager. The Device Manager page is displayed.

---

Device Manager

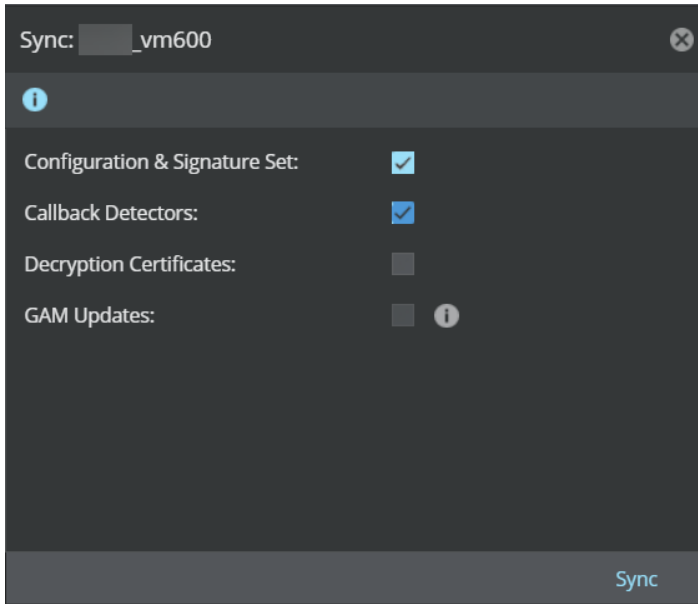



2. Click Sensors tab. Select the required Sensor from the list.
3. Select Sync.  
The Sync: <Device Name> window is displayed.
4. Select the required configurations and click Sync.

#### Note

The Manager provides an option to concurrently deploy pending changes for multiple Sensors. When you select multiple Sensors for deployment, the Bulk Sync window is displayed and enables all check-boxes by default. Select the options you wish to deploy and click Sync.

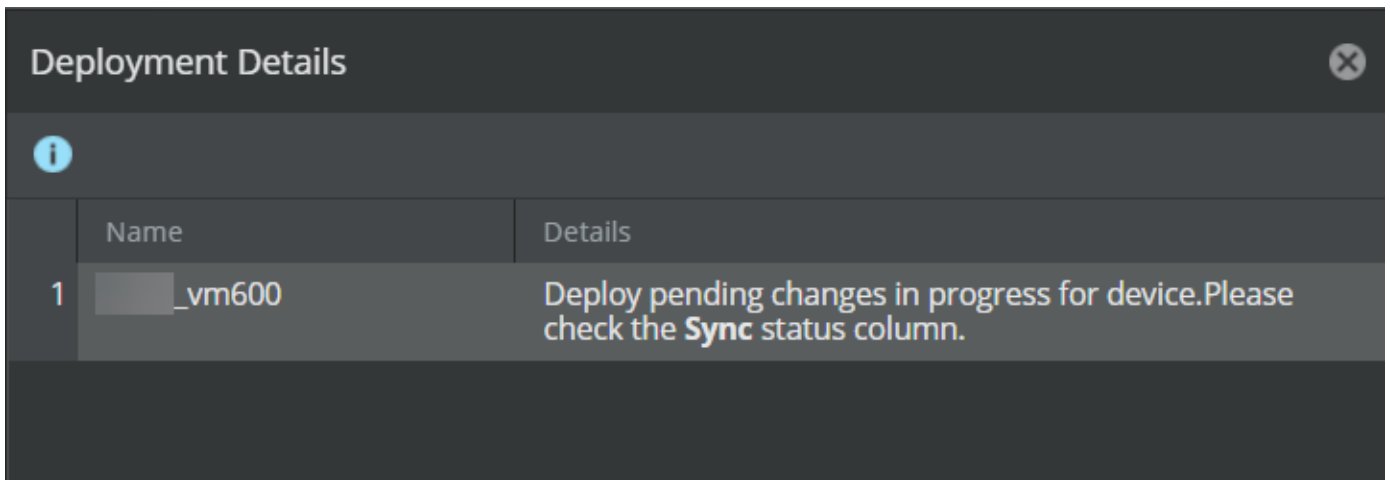
Sync: <Device Name> window



A Deployment Details dialog box is displayed. Click .

---

#### Deployment Details



You can also deploy the changes to a specific device from Devices <Admin Domain Name> Devices <Device Name> Deploy Pending Changes. Select the required configurations and click Deploy.

---

Device-level deploy pending changes


Deploy Pending Changes						
Device Name	Last Deployment	Pending Changes	Configuration & Signature Set	SSL Key	Callback Detectors	GAM Updates
_vm600	2022-Jun-30 10:38:38 IST	Policy Changed Global Policy Changed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[Deploy](#)

The following status can be viewed from Sync section of Status column:

Status	Description
Synchronized	Indicates that no pending changes are required.
Sync in progress	Indicates when the deployment is in progress.
Sync required	Indicates if any pending changes are required.
---	Indicates that there is no trust established between the Sensor and the Manager.

5. Click Export Sync File under Other Actions to view and export the deployment changes file to indirect mode Sensors. The changes can then be deployed to the Sensors manually using the CLI command window.

6. Click  to refresh the page and the status of the deployment.

:

## Update the latest software images on all devices

You can download the available Sensor software updates on demand from Manager → <Admin Domain Name> → Trellix IPS Protection Status. Select Device Software tab. Then, select Download Device Software. If more than one version is available for download, select the most recent version. For example, if multiple versions, such as 11.1.1.4, 11.1.1.5, and 11.1.1.6 are available for download, Trellix recommends you download version 11.1.1.6. The latest version of software always contains the changes included in all previous releases. If needed, you can also downgrade your Sensor by choosing from the list of available versions.

The Manager allows you to simultaneously download software images to all your Sensors listed under the Devices node. The Manager also provides an option to concurrently perform the Sensor upgrade by selecting the specific Sensor under Devices → <Admin Domain Name> → Devices → <Device Name> → Maintenance → Deploy Device Software. For Sensors in a stack, select Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Maintenance → Deploy Device Software.

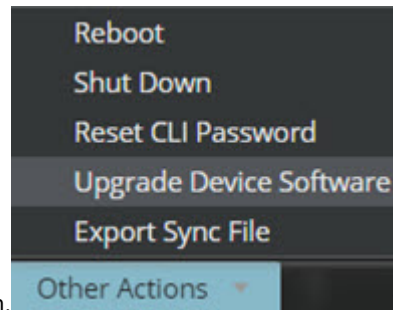
### Note

Once the software is updated in the Sensor, you must reboot all updated Sensors.

To download a software update, do the following:

#### Steps:

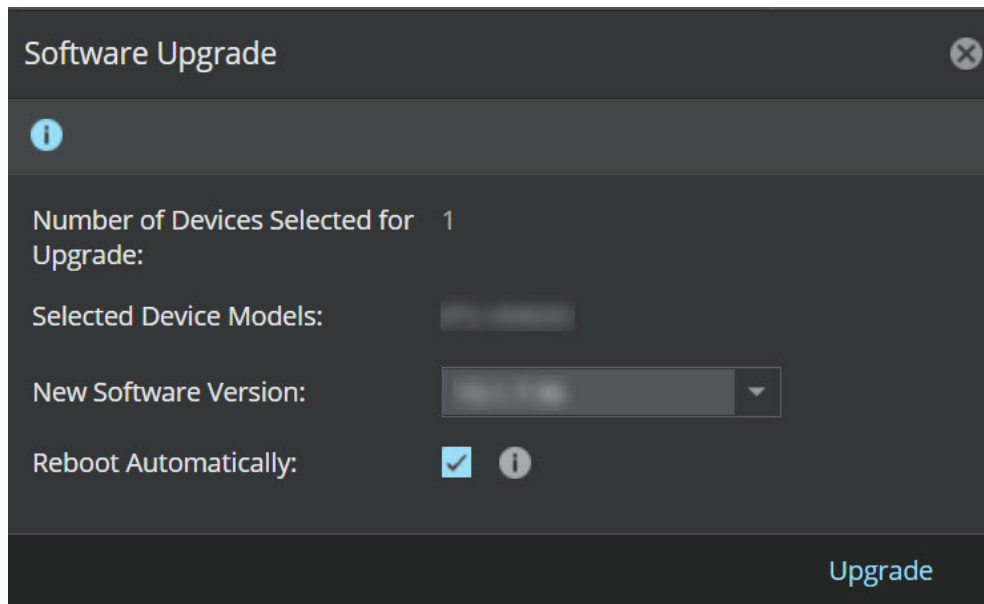
1. Go to Devices → <Admin Domain Name> → Global → Device Manager.  
The Device Manager page is displayed.
2. Select the Sensors tab.
3. From the list, select the required Sensor. The Manager also provides an option to concurrently perform the software upgrade for multiple Sensors using same model and software version.



4. Select Upgrade Device Software from Other Actions drop-down. The Software Upgrade dialog box is displayed.

---

Software Upgrade dialog box



---

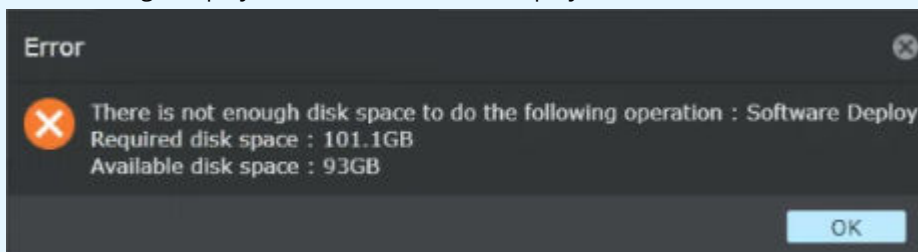
5. Select the New Software Version to be downloaded to the Sensor from the drop-down.

 **Note**

- You can only view the downloaded device software versions.
- The Manager reserves 100 GB under required free disk space for Manager operations and considers an additional file size of 1.2 GB to be generated for each software deployment request. Upon receiving the request (single or in bulk), it checks the number of Sensors selected, and calculates the free disk space. If there is insufficient free disk space, an error message is displayed in the UI stating the available disk space and the space required to complete the upgrade task. This enables the Manager to reserve sufficient disk space to keep other processes running and avoid any software upgrade failure scenario.

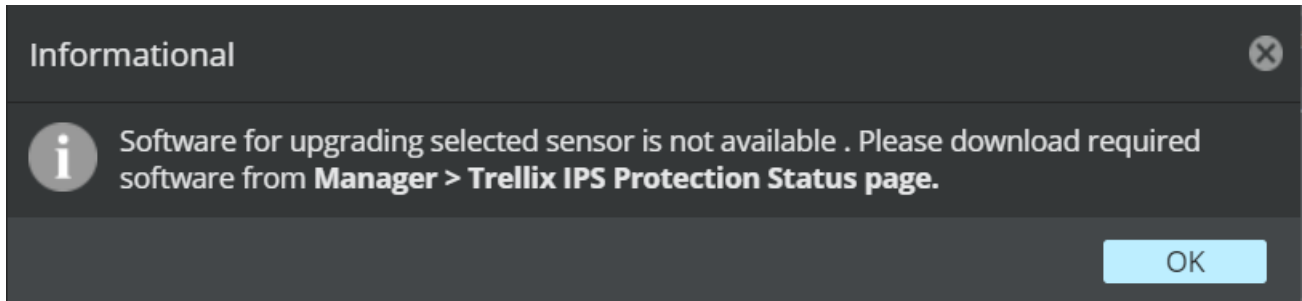
---

Error message displayed for device software deployment if there is insufficient disk space





For the Sensor, if required software version is not downloaded in the Manager, an Informational dialog box is displayed.

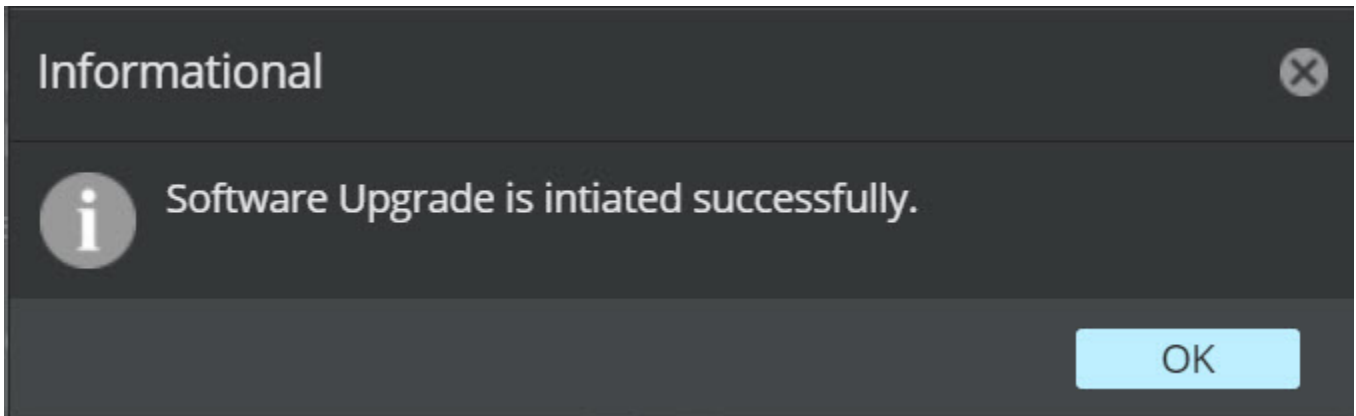


6. To automatically push the Sensor for reboot, enable Reboot Automatically.



 **Note**


By default this option is enabled. If required, it can be disabled.  
 For NS-series Sensors, you must do a full reboot as hitless reboot is not supported when SSL decryption is enabled.

7. Click the Upgrade to initiate the process. An Informational dialog box is displayed to provide the status update. Click OK.



The Last Upgrade section of Device Details column provides the time stamp of last upgrade performed. To view the software upgrade status, go to Upgrade Status section of Device Details column. You can also view the status from Background Tasks tab of Manager → <Admin Domain Name> → Troubleshooting → Logs. The following statuses are displayed:

Status	Definition
 Successful	When the Sensor upgrade is successful.
	When the Sensor is upgrading to the latest software version.

Status	Definition
In-progress	
 Failed	When the Sensor upgrade fails.
---	When no upgrade is performed.

8. The Export Sync File from Other Actions drop-down is used to update and export files for offline Sensors.

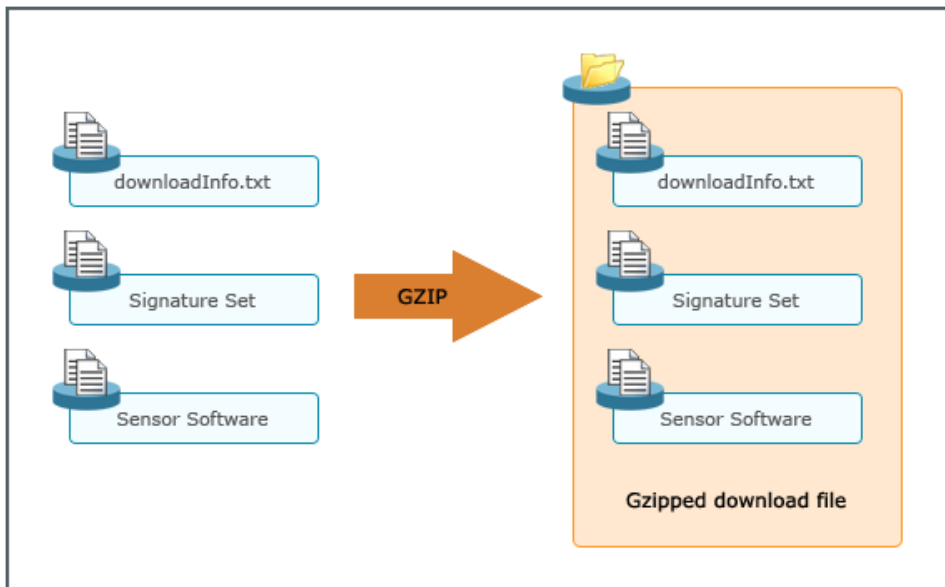
:

### 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:

Encryption process



:


### Configure a new device for indirect mode 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 deployment mechanism while adding a new device. By default, all devices added to the Manager have the deployment mode as Direct. Devices with Direct mode 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 Indirect. If required, you can edit the deployment mode later.

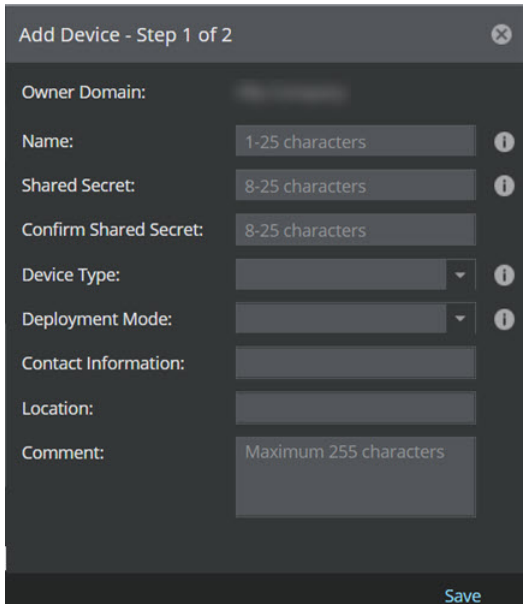
Follow this procedure to configure a new device for Indirect update:

#### Steps:

1. Go to Devices → <Admin Domain Name> → Global → Device Manager.  
The Device Manager page is displayed.
2. Select the Sensors tab and click . The Add Device - Step 1 of 2 panel is displayed.
3. Enter a device name against Name.
4. Provide Shared Secret details.
5. Confirm the Confirm Shared Secret details.
6. Select IPS Sensor against Device Type drop-down.
7. Select Indirect against Deployment Mode drop-down and click Save.

---

Add Device - Step 1 of 2 window



The screenshot shows a dark-themed configuration window titled "Add Device - Step 1 of 2". It contains the following fields and controls:

- Owner Domain: [Text input]
- Name: [Text input, 1-25 characters]
- Shared Secret: [Text input, 8-25 characters]
- Confirm Shared Secret: [Text input, 8-25 characters]
- Device Type: [Dropdown menu]
- Deployment Mode: [Dropdown menu]
- Contact Information: [Text input]
- Location: [Text input]
- Comment: [Text input, Maximum 255 characters]

A "Save" button is located at the bottom right of the window.

The device is configured for Indirect updates.

### Note

The Deployment Mode configured on the Primary device of the Fail-Over Pair determines the signature file generation for download.

### Note

If the Deployment Mode for the Primary device is configured as Indirect, two individual signature files are generated for Primary and Secondary devices, irrespective of the Secondary device configuration.

### Note

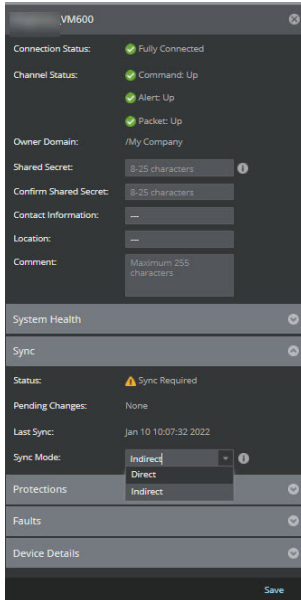
If the Deployment Mode for the Primary device is configured as Direct, the signature file is downloaded Direct to both the devices, irrespective of the Secondary device configuration.

## : **Configure an existing device for indirect mode signature set update**

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

### Steps:

1. Go to Devices → <Admin Domain Name> → Global → Device Manager.  
The Device Manager page is displayed.
2. Select the Sensors tab to view the list of devices configured.
3. Double click on the required Sensor. The <Device Name> details panel is displayed.



4. Scroll to the Sync section. Select Indirect against Sync Mode drop-down and click Save.

### Note

You can also change the configured mode in Summary page. For standalone Sensors, go to Devices → <Admin Domain Name> → Devices → <Device Name> → Summary. For Sensors in Stack, go to Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → Stackname-node id → Summary. In the Summary page, go to Sync monitor and select Indirect against Sync Mode drop-down and click Save.

5. An information box confirms a successful edit. The device is configured for Indirect updates.

:

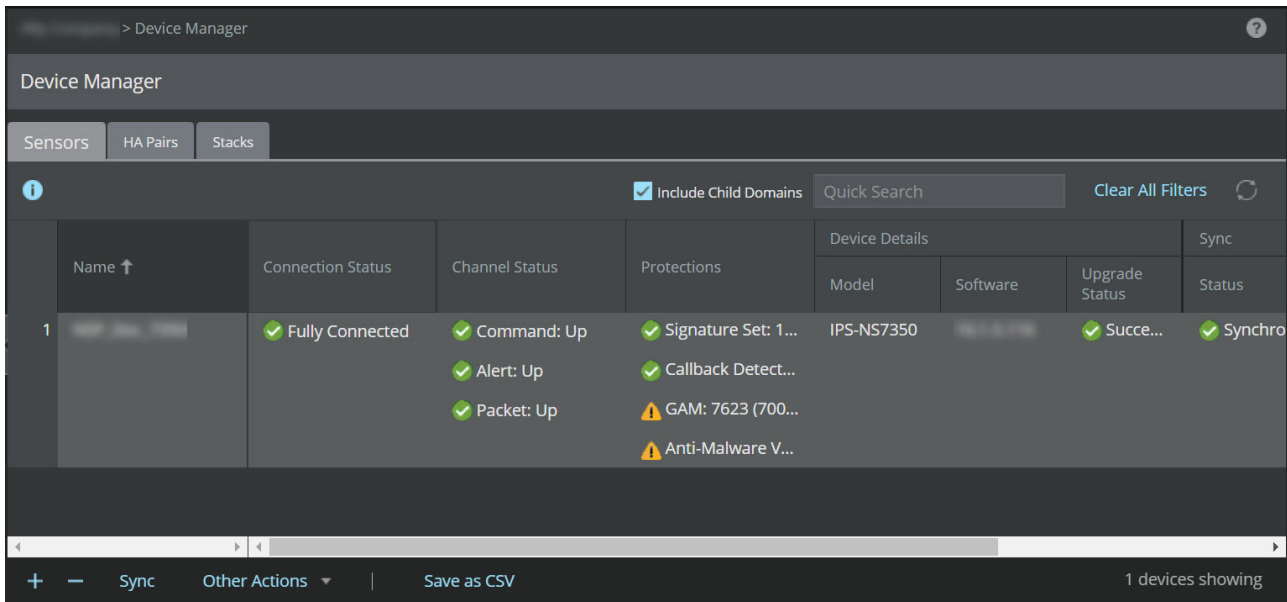
## Update configuration for offline devices

Follow this procedure for updating device configuration for offline devices:

### Steps:

1. Go to Devices → <Admin Domain Name> → Global → Device Manager.  
The Device Manager page is displayed.

2. Select the Sensors tab. From the list, select required Sensor.



3. Select Export Sync File from Other Actions drop-down.
4. Save the device configuration file to the location of your choice.
5. Copy the device configuration file to the TFTP server.
6. Connect to the device through CLI and configure the TFTP server IP.
7. Execute the **loadconfiguration <device configuration filepath in the tftpserver><device configuration filename>** command.
8. Once the device configuration file is copied on to the device, check with **downloadstatus** command in the CLI to get the status.

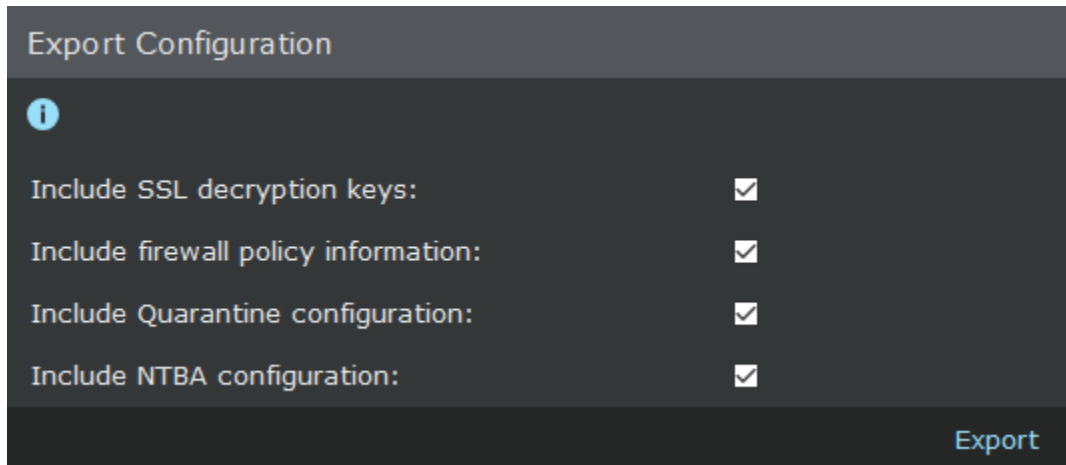
:

## Export device configuration

Follow this procedure to export a device's configuration to a file:

### Steps:

1. Click Devices → <Admin Domain> → Devices → Maintenance → Export Configuration .The Export Configuration page is displayed.



2. Select the relevant checkboxes, click Export, and save the file in the desired location in the local machine.

:

To perform an offline download of the signature set:

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.

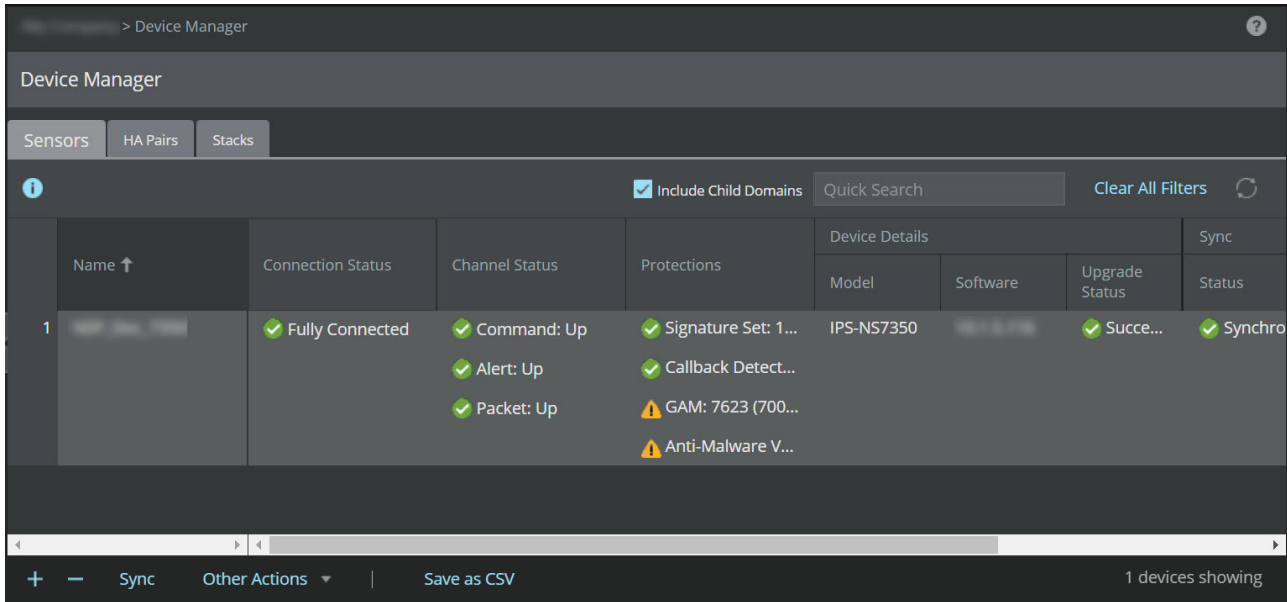
:

### Update software for offline devices

Follow this procedure for updating device configuration for offline devices:

**Steps:**

1. Go to Devices → <Admin Domain Name> → Global → Device Manager. The Device Manager page is displayed.



2. Select the Sensors tab. From the list of Sensors, select the required Sensor.
3. Select Export Sync File from the Other Actions drop-down.
4. Save the device image upgrade file to the location of your choice.
5. Copy the device configuration file to the TFTP server.
6. Connect to the device through CLI and configure the TFTP server IP.
7. Execute the `loadconfiguration <image filepath in the tftp server><imagefile name>` from the CLI.
8. Once the image file copied on to the device (it takes some time), check with `downloadstatus` command in the CLI to get the status.
9. Reboot the device on successful loading of the image.

### Note

You can perform Sensor reboot by clicking Reboot from Other Actions drop-down.

:

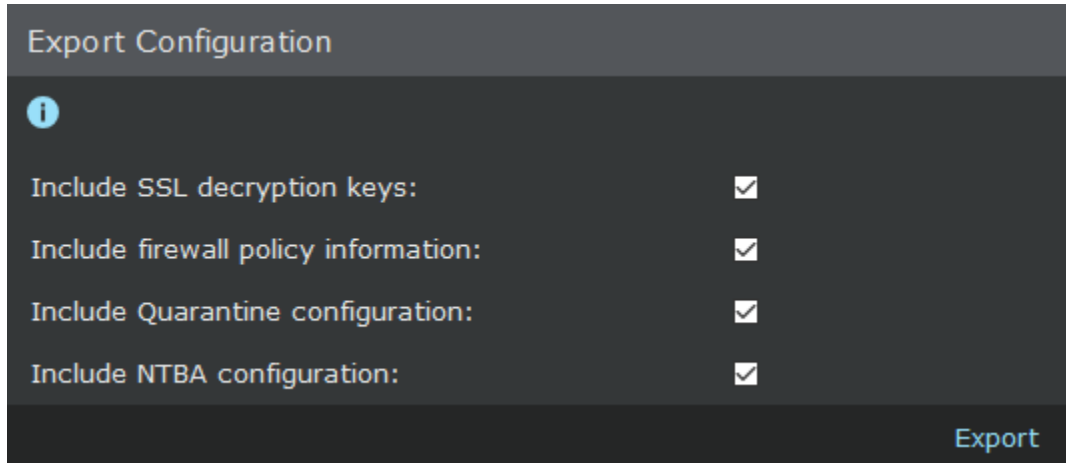
## Export device configuration

Follow this procedure to export the selected device's configuration to a file:

### Steps:

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





2. Select the configuration options that you wish to export, click Export, and save in the desired location

:

To perform an offline download of the device software:

### Steps:

1. Set up the Manager and device.
2. Import the device image jar file on to the Manager from Manual Import tab, using Manager → <Admin Domain Name> → Trellix IPS Protection Status.
3. Go to Devices → <Admin Domain Name> → Global → Device Manager.  
The Device Manager page is displayed.
4. Select the Sensors tab. From the list, select the required Sensor.
5. Select Export Sync File from Other Actions drop-down.
6. Save the device image upgrade file to the location of your choice.
7. Copy the device configuration file to the TFTP server.
8. Connect to the device through CLI and configure the TFTP server IP.
9. Execute the **loadconfiguration <image filepath in the tftp server><imagefile name>** from the CLI.
10. Once the image file copied on to the device (it takes some time), check with **downloadstatus** command in the CLI to get the status.
11. 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 Block list can be updated through the intervention of the security administrator. Updates for these engines can be carried out independently irrespective of the Sensor software version.

However, for Gateway Anti-Malware, you must be aware of the versions of the malware engines that are compatible with specific Sensor and Manager versions. Refer to Gateway Anti-Malware Engine in the section *How an Advanced Malware policy works* in *Trellix Intrusion Prevention System Product Guide*.

### Gateway Anti-Malware Engine for an airgap network

The Gateway Anti-Malware engine initialization in the Sensors requires an active connection to the GTI server. If your Sensors are in a network without an active GTI connection, the Gateway Anti-Malware engine initialization in the Sensor fails. In such a scenario, you must enable the airgap mode of Gateway Anti-Malware to initialize the Gateway Anti-Malware engine. You can achieve this by executing the **set gam-airgap-network enable** command in the Sensor CLI and reboot the Sensor for the changes to take effect.

For example, you can configure the Sensors to initialize the Gateway Anti-Malware engine in airgap mode when your network meets the following conditions:

1. The Sensors are in a private network.
2. You cannot use the Public GTI server.
3. You do not have a Private GTI server.

You must enable the airgap mode of Gateway Anti-Malware before pushing the updates from the Manager to the Sensor. To view the status of the Gateway Anti-Malware updating for an airgap network, execute the **show gam-airgap-network status** command in the Sensor CLI.

#### Note

The Gateway Anti-Malware engine initialization for the Sensors in airgap network is supported on Gateway Anti-Malware 2019 version 0 and later.

:

### 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 in the subsequent sections.

#### Note

The deployment of Gateway Anti-Malware Engine is not supported on Virtual NTBA devices.

:

### Prerequisites:

- 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 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 200 MB.

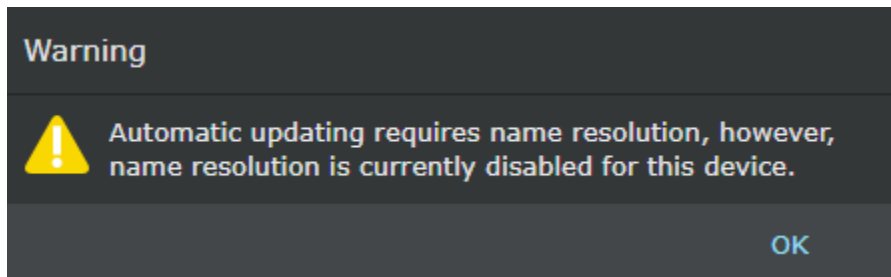
You can set up automatic updates for both these components using these steps. If you do not want to set up automatic updates, you can use the existing process for manual updates.

### Steps:

1. Click Devices → <Admin Domain Name> → Global → Common Device Settings → GAM Updating.  
The GAM Updating page appears.
2. Select Enable Automatic Updating?.

---

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 Trellix 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.

:

### Prerequisites:

- 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 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 200 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.

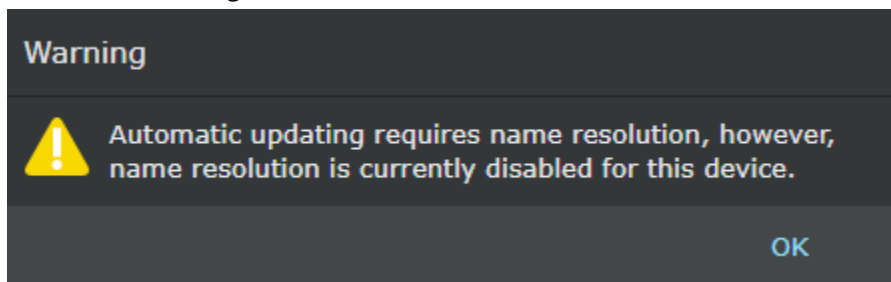
This page displays a grid that mentions the active version and latest available version of each component. If you are using the latest version the circle is green. If a newer version is available, the circle is colored red.

### Steps:

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?.

---

Notification to configure a DNS server

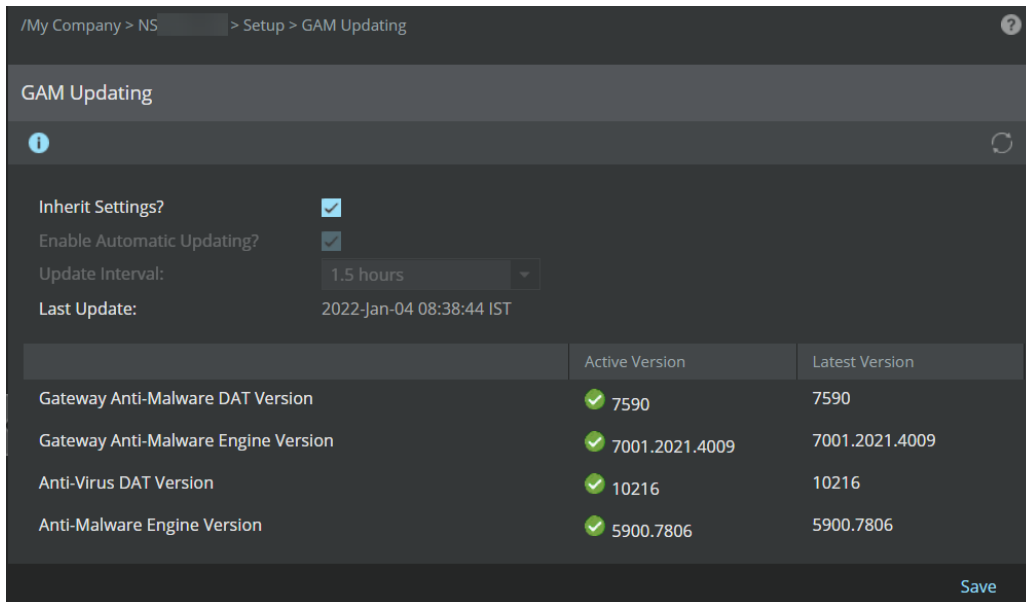


If you have not configured a DNS server for this device, you will receive a notification prompting you to do so.

4. Click the Update Interval drop-down. The range of the update interval is between 1.5 hours and 24 hours since Trellix provides updates several times in a day.
5. Click Save to complete the configuration.

---

GAM Updating page shows versions for individual items



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

:

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.

When the Gateway Anti-Malware engine is enabled for the first time, the engine is in uninitialized state when integrated with a Private GTI cloud. To receive a manual update, the Gateway Anti-Malware engine has to be in initialized state. To initialize the engine, the Sensor has to be online and connected to the Private GTI server to receive the update for the first time. Once the Gateway Anti-Malware engine is initialized after receiving the update from Private GTI server, you can push the updates to the Sensor. For subsequent manual Gateway Anti-Malware engine update, you can download the update and import it to the Manager.

### Note

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 in the section *How an Advanced Malware policy works* in *Trellix Intrusion Prevention System Product Guide*.

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

### Steps:

1. Select Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Name Resolution.

The DNS server is configured for the Sensor to reach the GTI server.

- Using a recent version of your browser, go to the Gateway Anti-Malware Update Server URL: <https://contentsecurity.skyhigh.cloud/UPDATE>.
- On the page that appears, review the terms and conditions and select the I accept the terms and conditions check-box, and click Next Step.

---

Accept License Agreement

## Manual Update

---

### Download Update Package

If you have a valid licensed product you can manually download personalized update packages. These update packages can be used for a manual import into your 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 DAT updates, are intended only for Skyhigh Security customers with a valid Technical Support Agreement.

I accept the terms and conditions

Next Step

---

You are routed to the next page where you will need to select the appropriate Trellix product.

- On this page, click the drop-down to select Trellix Intrusion Prevention System, and click Next Step.

---

Select update package

## Manual Update

---

### Download Update Package

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

#### Step 2/4

Please select your product

Trellix Intrusion Prevention System

---

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

5. Under step 3:
  - a. For "Trellix Intrusion Prevention System" version, enter **11.1** if your Sensor runs on 11.1.5.x version, or enter **10.1** if your Sensor runs on 10.1.5.x version.
  - b. For "Trellix Intrusion Prevention System" build number, enter **11.1.5.x** if your Sensor runs on 11.1.5.x version, or enter **10.1.5.x** if your Sensor runs on 10.1.5.x version.
  - c. Click Next Step.

---

Specify version and build number

## Manual Update

### Download Update Package

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

#### Step 3/4

"Trellix Intrusion Prevention System" version

"Trellix Intrusion Prevention System" build number

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.

Gateway Anti-Malware engine compatibility matrix

Manager	Sensor	Gateway Anti-Malware engine version downloaded	What you must enter...
10.1.7.55 or later	10.1.5.153 or later	2021	You must enter the Sensor software version as 10.1.5.x.
10.1.7.29 or later	10.1.5.41 or later	2019 version 0	You must enter the Sensor software version as 10.1.5.x.
10.1.7.4 or later	10.1.5.3 or later	2017 version 2	You must enter the Sensor software version as 10.1.5.x.



6. Click Generate Update Package.

---

Generate Update Package

## Manual Update

---

### Download Update Package

If you have a valid licensed product you can manually download personalized update packages. These update packages can be used for a manual import into your 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

- Gateway Antimalware (~340+ MB)

- 
7. Click Download and save the package to a convenient location.

---

Download Update Package

## Manual Update

### Download Update Package

Your personalized update package is valid for the following product:

- Trellix Intrusion Prevention System Version 10.1 Build 10.1.5.
- Linux (x86\_64)
- Included Updates
  - Gateway Antimalware

Personalized Update Package	
Filename	ips-linux-antimalware.upd
Filesize	175 MB
MD5 Checksum	1746ff0dbee7f579e75455f4da5c21ae
SHA1 Checksum	64ac830f3f683de79010b93a9261893341f13e06
SHA256 Checksum	e941f69ad87df14186c2ee6ff9d3bbb0bc5973dd660c0703348ae8589997599e
Date	

After the package is generated, you are shown details about the file such as filename, file size, MD5, SHA1, SHA256 checksums and date.

- After the file is downloaded, log on to the Manager and go to Manager → <Admin Domain Name> → Trellix IPS Protection Status. Select Manual Import tab. The Manual Import tab is displayed.
- In the Manual Import tab, click Browse, navigate to the file location, and select it.
- Select the file and click Import.  
A pop-up opens giving you the status of the upload.
- If you have configured auto-deployment of new GAM updates on the GAM Automatic Deployment tab under Manager → <Admin Domain Name> → Trellix IPS Protection Status, the imported GAM file will be deployed automatically on all the attached Sensors at once at the scheduled time. You can check the deployment status on the User Activities tab under Manager → <Admin Domain Name> → Troubleshooting → Logs. For detailed information on how to configure and schedule auto-deployment of GAM updates, refer to the section *Automatic deployment of GAM updates* in *Trellix Intrusion Prevention System Product Guide*.

### Note

The automatic deployment of GAM updates is not applicable to NTBA or virtual NTBA devices.

Or,

- After the file upload is complete, go to Devices → <Admin Domain Name> → Devices → <Device Name> → Deploy Pending Changes.

In the Deploy Pending Changes page, the Pending Changes column displays New Gateway Anti-Malware Versions.

13. Select the check-box for GAM Updates and click Deploy.

A pop-up window appears showing you the status of the update. Upon successful deployment, click Close in the pop-up window.

## Note

If the update fails, it is likely that you have downloaded an incompatible version. Review the compatible versions and the combinations listed in the *Gateway Anti-Malware engine compatibility matrix* table to ascertain if you have downloaded the appropriate version.

There is an alternate way to deploy the GAM update file to your Sensor from the Device Manager page. To deploy:

1. Navigate to Devices → <Admin Domain Name> → Global → Device Manager and select Sensors tab. The Sensors tab is displayed listing all the attached Sensors.
2. Select the compatible Sensor on which you want to deploy the GAM update file, and click Sync.

Select Sensor to synchronize GAM Updates

Device Manager									
Sensors   HA Pairs   Stacks									
<input checked="" type="checkbox"/> Include Child Domains   Quick Search   Clear All Filters									
ID	Name	Connection Status	Channel Status	Protections	Device Details				
					Type	Model	Software	Upgrade Status	System Running Ca
1	_7350	Fully Connected	Command: Up Alert: Up Packet: Up	Signature Set: 10.9.31.1 Callback Detectors: 3132 GAM: 7658 (7001.2021.4009) Anti-Malware Version: 10285 (5900.7806)	IPS Sensor	IPS-NS7350	10.1	---	---
2	_NS9200	Fully Connected	Command: Up Alert: Up Packet: Up	Signature Set: 10.9.31.1 Callback Detectors: 3132 GAM: 6911 (7001.2017.3112) Anti-Malware Version: 9439 (5900.7806)	IPS Sensor	IPS-NS9200	10.1	---	---

3. The Sync: <Device Name> window is displayed with GAM Updates check-box selected. If there are any other pending deployments, the respective check-boxes will also be selected by default. You may uncheck any of them if you want to skip their deployment.

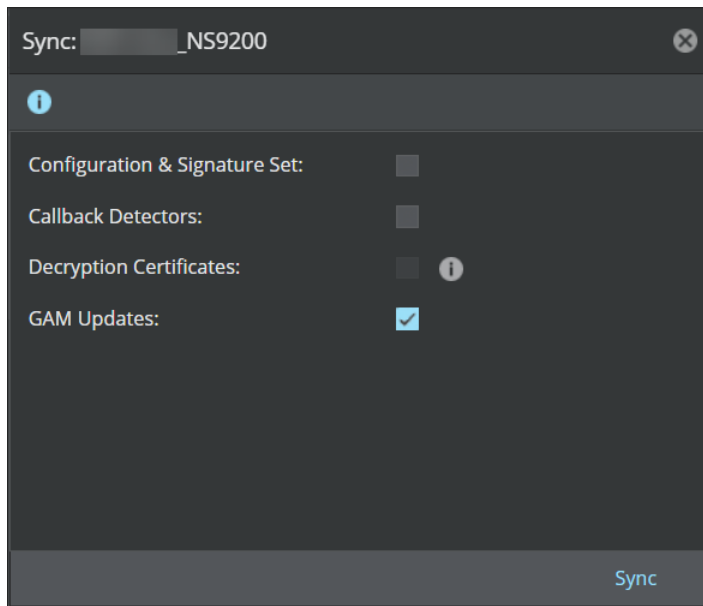
### Note

The Manager provides an option to concurrently deploy pending changes onto multiple Sensors. When you select multiple Sensors for deployment, a Bulk Sync window is displayed with all check-boxes selected by default. You may uncheck any of them if you want to skip their deployment.

4. Click Sync to begin the deployment.

---

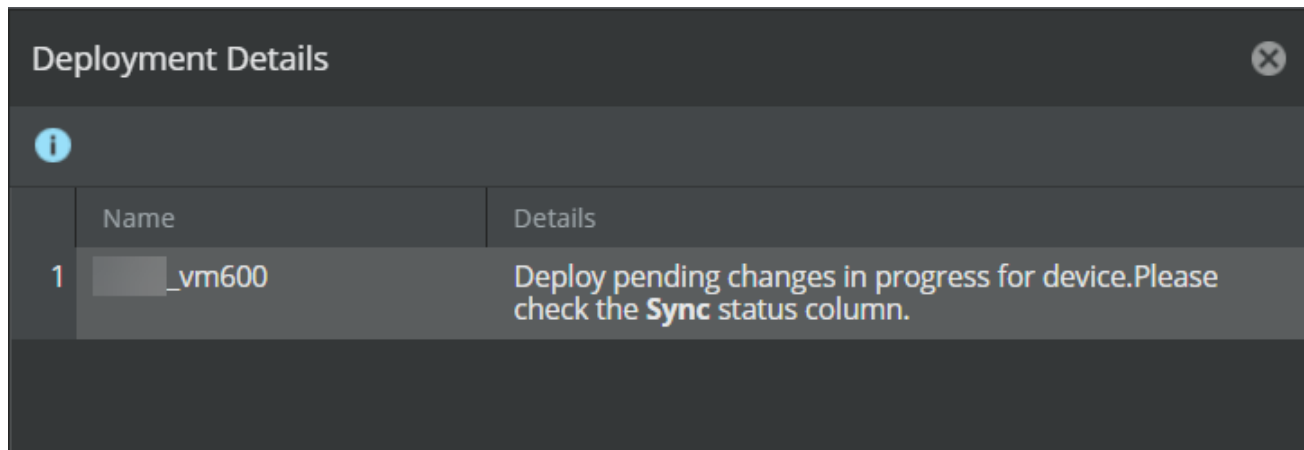
GAM Updates selected for synchronization




5. A Deployment Details dialog-box is displayed, click .

---

Deployment Details



6. You may click the  icon to refresh the Sensors tab and view the latest Sync status. Upon successful deployment, the status is displayed as Synchronized, and the deployed version of GAM is displayed under the Protections column.

#### Note

You can also view the deployment status in Manager → <Admin Domain Name> → Troubleshooting → Logs under the Background Tasks tab. The status is displayed as In Progress during the deployment and Complete upon successful deployment. You need to refresh the tab to view the latest deployment status.

#### Note

If the Sync fails, it is likely that you have downloaded an incompatible GAM version. Review the compatible versions and the combinations listed in the *Gateway Anti-Malware engine compatibility matrix* table to ascertain if you have downloaded the appropriate version.

:

## Manage HA pairs

Go to Devices → <Admin Domain Name> → Global → Device Manager page. You can add new HA pairs by selecting the HA pair tab. A HA pair will be managed just as any other device is managed, by going to Devices → <Admin Domain Name> → <Device Name> → Devices.

Using the HA Pairs tab, you can enable failover configuration for two identical Sensor models. The term "HA 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 HA 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).

### Note

For more information on high availability using HA pairing, see the *Trellix Intrusion Prevention System Product Guide*.

NS-series Sensor model	Port(s) used for failover
NS9500	G0/1 (QSFP28 100 or 40G QSFP+)
NS9300	G1/1 and G1/2 (40G QSFP+)
NS9200	G0/1
NS9100	G0/1
NS7500	G0/1
NS7350	G0/1 (10G SFP+)
NS7250	G0/1 (10G SFP+)
NS7150	G0/1 (10G SFP+)
NS7300	G0/1 (10G SFP+)
NS7200	G0/1 (10G SFP+)
NS7100	G0/1 (10G SFP+)

NS-series Sensor model	Port(s) used for failover
NS5200	G1/1 and G1/2
NS5100	G1/1 and G1/2
NS3500	Not Supported
NS3200/NS3100	1

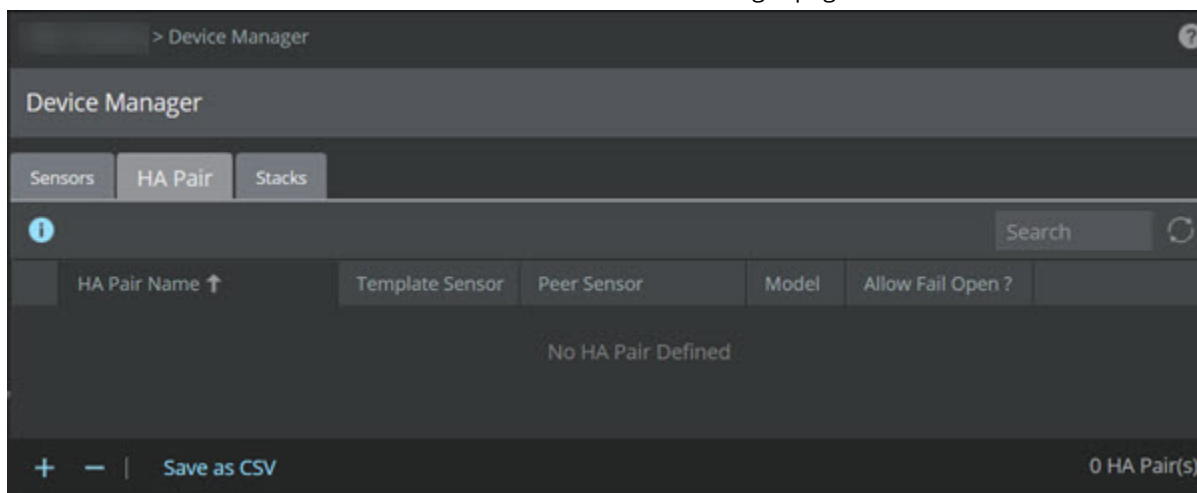
 **Note**

High availability is not supported in NS3500 Sensor.


To configure two devices for failover, do the following:

**Steps:**

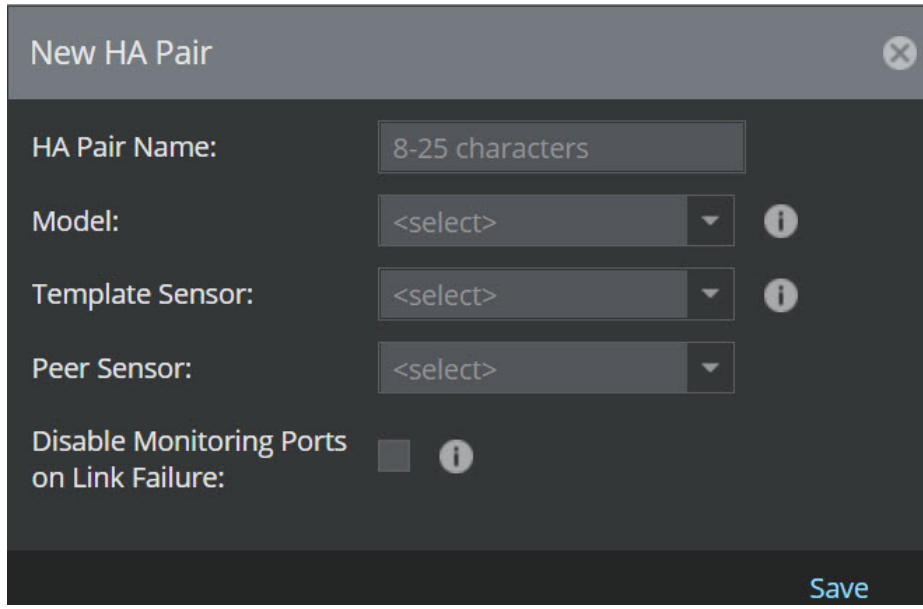
1. Go to Devices → <Admin Domain Name> → Global → Device Manager page and select HA Pairs tab.



The HA Pairs tab is displayed.

2. Click . The New HA Pair dialog box is displayed.

New HA pair window



3. Enter the HA pair name that will uniquely identify the grouping in HA Pair Name.
4. Select the Model from the drop-down option. Both devices in a HA pair must be using same model and same version.
5. Select the Template Sensor from the drop-down option.
6. Select the Peer Sensor from the drop-down option.
7. Enable or disable Disable Monitoring Ports on Link Failure for the HA pair as per your requirement. By default, it is disabled.
8. Click Save. A Confirmation dialog box is displayed. Click OK. The new HA pair will appear in the display list.

#### Note

In the Manager, if at least two Sensors are not using same model and software version, an Error dialog box is displayed.

#### Note

An option to edit the existing HA pair is not provided. If you double-click a row in the grid, an Error dialog box is displayed. You change the configuration by deleting and re-creating a HA pair.

#### Note

If you have created a HA pair while maintaining an open Attack Log window, the Attack Log 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 HA 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 HA pair as the identifying device.) Restart the Attack Log for proper alert reporting. The same is true in reverse if a HA pair is deleted. You must restart the Attack Log to view alerts separately from each device.



:

## 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 IP Reputation.

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

### Note

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

### Note

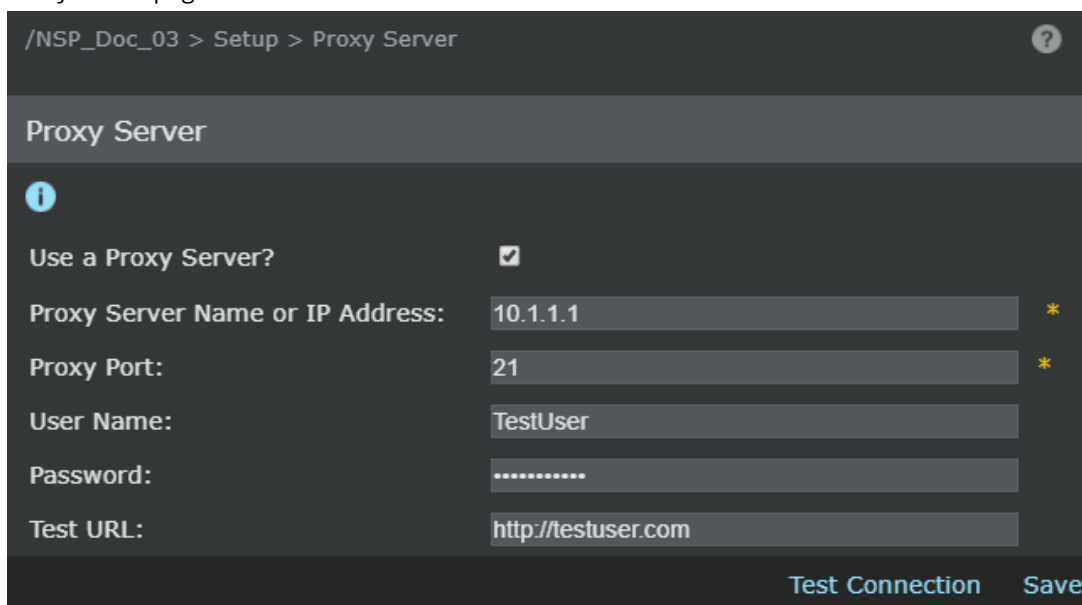
SOCKS, a network-level proxy, is not currently supported by Trellix IPS.

Follow this procedure to specify your proxy server:

### Steps:

1. Select Manager → <Admin Domain> → Setup → Proxy Server. The Proxy Server page is displayed.

Proxy Server page



The screenshot shows the 'Proxy Server' configuration page. At the top, the breadcrumb navigation is '/NSP\_Doc\_03 > Setup > Proxy Server'. Below the title 'Proxy Server', there is an information icon. The configuration fields are as follows:

Use a Proxy Server?	<input checked="" type="checkbox"/>	
Proxy Server Name or IP Address:	<input type="text" value="10.1.1.1"/>	*
Proxy Port:	<input type="text" value="21"/>	*
User Name:	<input type="text" value="TestUser"/>	
Password:	<input type="password" value="....."/>	
Test URL:	<input type="text" value="http://testuser.com"/>	

At the bottom right of the form, there are two buttons: 'Test Connection' and 'Save'.

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 User Name 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 for a domain

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, 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, there might be issues related to time difference while switching from NTP server to the Manager and vice versa.

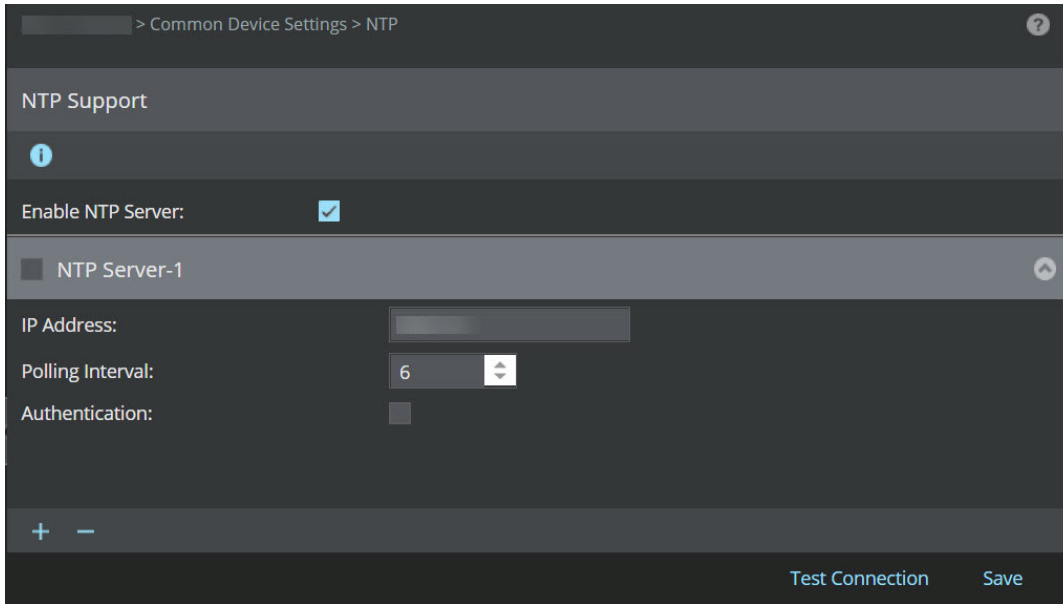
To specify your NTP server, do the following:

#### Steps:

1. Select Devices → <Admin Domain Name> → Global → Common Device Settings → NTP  
The NTP Support page appears.


---

Configure NTP servers



### Note

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. To configure the NTP Server click , NTP Server-<number> section is displayed.
  - 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 ID.
  - e. Select the required key from Authentication Key Type drop-down. This key can be MD5, SHA, or SHA1.

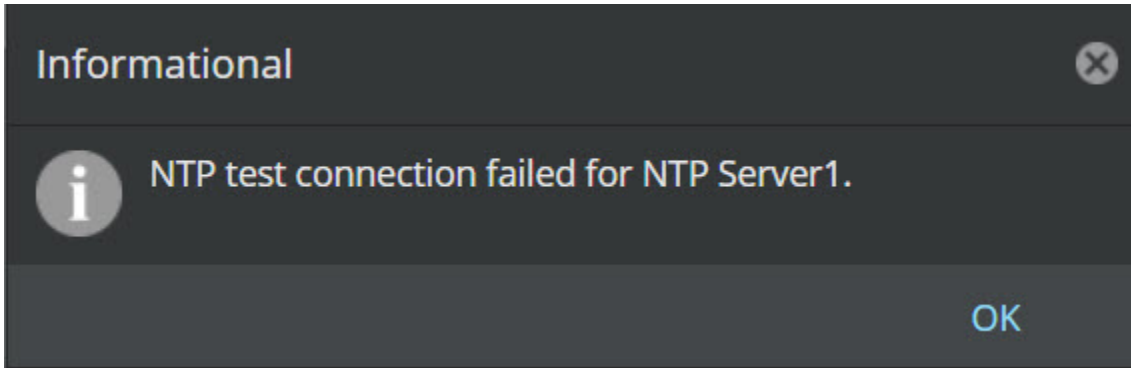
### Note

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. An Informational dialog box displays the status of connectivity test.

---

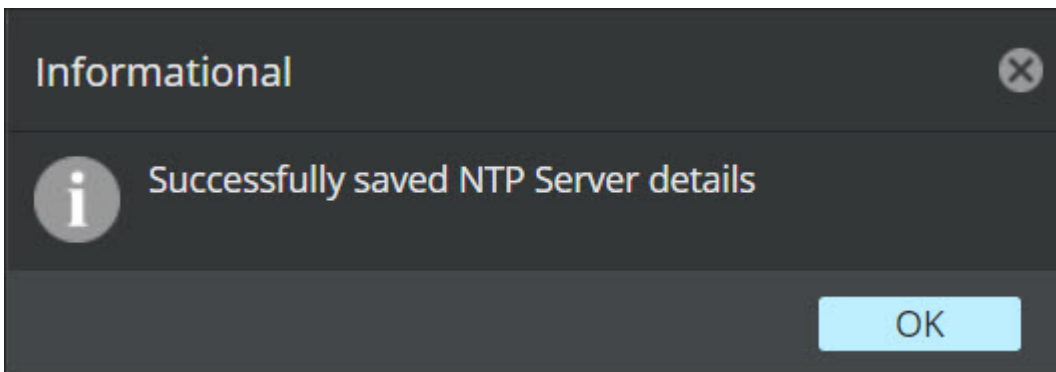
NTP: Test Connection notification



g. Click Save to save your settings. An Informational dialog box displays the status of configuration.

---

NTP: Save notification



 **Note**

- The Manager allows you to configure a maximum of two NTP servers with the same IP address format (i.e., IPv4 or IPv6). If you configure both NTP servers, NTP Server-1 takes a higher priority.
- The IPv4 and IPv6 addresses are mutually exclusive. For 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.

4. To remove any NTP server, select the checkbox beside NTP Server-<number> and click .

:

### 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, 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, there might be issues related to time difference while switching from NTP server to the Manager and vice versa.

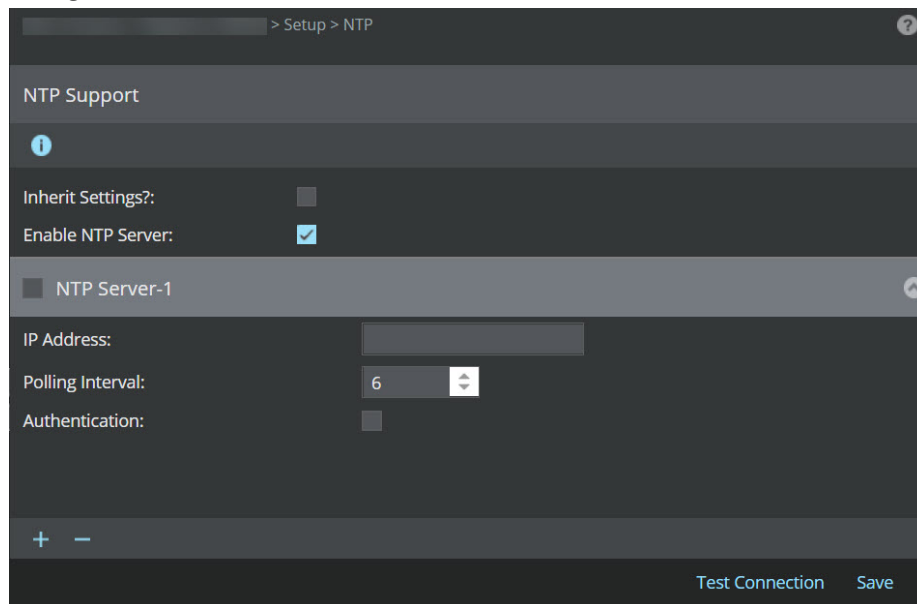
To specify your NTP server, do the following:

### Steps:

1. Select Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → NTP.

The NTP Support page appears.

### Configure NTP servers




The screenshot shows the 'NTP Support' configuration page. At the top, there is a breadcrumb trail '> Setup > NTP' and a help icon. Below the title, there is an information icon. The configuration options are: 'Inherit Settings?' with an unchecked checkbox, 'Enable NTP Server:' with a checked checkbox, and a section for 'NTP Server-1' with a collapse icon. Under 'NTP Server-1', there are fields for 'IP Address:' (with a text input), 'Polling Interval:' (with a spinner set to 6), and 'Authentication:' (with an unchecked checkbox). At the bottom of the section are '+' and '-' icons. At the very bottom of the page are 'Test Connection' and 'Save' buttons.

### Note

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

2. Deselect Inherit Settings? to override the configuration in the parent domain.

3. To enable communication with the NTP server, select Enable NTP Server? To stop NTP from the Manager, unselect this option.

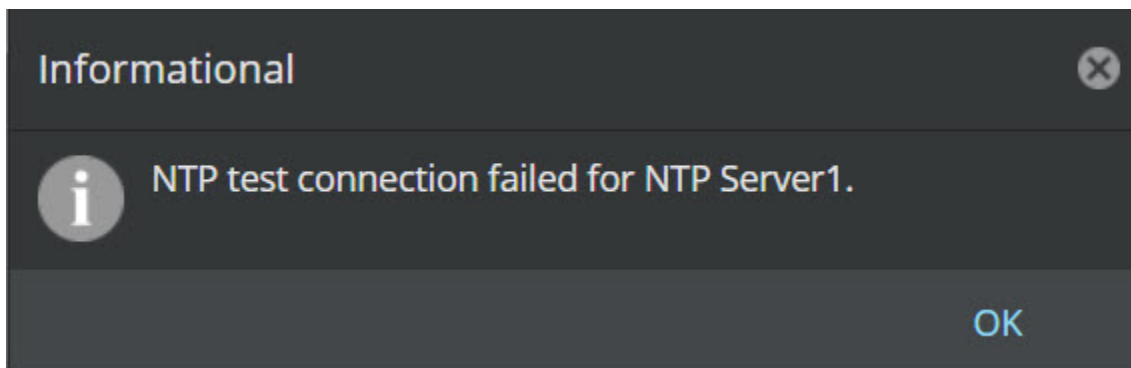
4. To configure the NTP Server click , NTP Server-<number> section is displayed.
- Type the IP Address. This can be an IPv4 or IPv6 address.
  - Enter the Polling Interval. The range is 3 ~ 17. The configured polling interval is applied as  $2^x$  seconds (2 power x).
  - Select Authentication to enable authenticating the NTP servers.
  - Enter the Authentication Key ID.
  - Select the required key from Authentication Key Type drop-down. This key can be MD5, SHA, or SHA1.

### Note

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

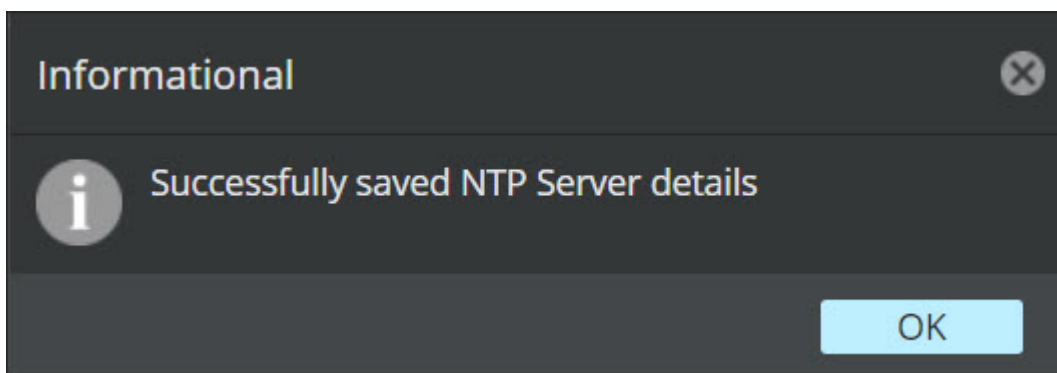
- f. Click on the Test Connection button to check the connectivity to the NTP server. An Informational dialog box displays the status of connectivity test.

NTP: Test Connection notification



- g. Click Save to save your settings. An Informational dialog box displays the status of configuration.

NTP: Save notification



### Note

- The Manager allows you to configure a maximum of two NTP servers with the same IP address format (i.e., IPv4 or IPv6). If you configure both NTP servers, NTP Server-1 takes a higher priority.
- The IPv4 and IPv6 addresses are mutually exclusive. For 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.

5. To remove any NTP server, select the checkbox beside NTP Server-<number> and click .

:

## 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, and 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 *Trellix Intrusion Prevention System Product Guide*.

### Note

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

The <Device\_Name> page for a Sensor in general contains Summary, Setup, Maintenance, Troubleshooting, Deploy Pending Changes, and IPS Interfaces pages.

:

## 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 details of a specific device.

- 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

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.

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 Sensors from Manager → <Admin Domain Name> → Trellix IPS Protection Status. Select Signature Sets tab. The Signature Sets tab is displayed. Schedule the frequency at which the automatic deployment must occur by enabling the Automatically Deploy New Signature Sets option from Automatic Deployment (Manager to Devices). The configurations are automatically deployed to Sensors from Manager based on schedule.

All configurations in the Policy page that apply to your Sensors can also be manually pushed from Devices → <Admin Domain Name> → Global → Device Manager. Select Sensors tab. From the list, select the required Sensors. Select Sync (all Sensors in a domain) or Devices → <Admin Domain Name> → Devices → <Device Name> → Deploy Pending Changes (to a single Sensor) action.

#### Scheduled deployment

##### Steps:

1. Select Manager → <Admin Domain Name> → Trellix IPS Protection Status. Select Signature Sets tab. The Signature Sets tab is displayed.

---

Automatic Deployment (Manager to Devices)



2. Enable Automatically Deploy New Signature Sets? option. By default, it is disabled.

- To push signature sets update to all Sensors immediately after it is downloaded to the Manager, select Immediate (after download) from Deployment drop-down. Click Save to setup the automatic deployment.
- To configure the required interval of automatic deployment, select Scheduled from Deployment drop-down option. Choosing this provides, When option.
- From the When option, customize the interval at which the deployment must occur. The following options are displayed in the drop-down list:
  - Daily: To deploy new signature sets daily. Set the time at which the deployment must occur.
  - Weekly: To deploy new signature sets weekly. Set the day of the week and time at which the deployment must occur.
  - Custom: To customize the interval at which the deployments must occur. The following options are displayed:
    - Every: Set the recurrence of time for the devices to poll the Manager.
    - Between: Set the time range at which the deployment must occur.

3. Click Save.

### On-demand deployment

#### Steps:

1. Select Devices → <Admin Domain Name> → Devices → <Device Name> → Deploy Pending Changes.  
The Deploy Pending Changes page is displayed.

Deploy Pending Changes page

Deploy Pending Changes						
Device Name	Last Deployment	Pending Changes	Configuration & Signature Set	SSL Key	Callback Detectors	GAM Updates
NSP_Doc_NS7100	2019-Sep-12 12:39:51 IST	Configuration Changed Global Policy Changed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. View the update information. If changes have been made, the Configuration & Signature Set column is checked by default.
3. Click Deploy. A pop-up window displays configuration download status.

:

### Update software for a Sensor

The Upgrade action enables an on-demand download of the latest or earlier software updates for a Sensor 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.

#### Note

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

#### Note

For example, if multiple versions, such as 10.1.1.4, 10.1.1.5, and 10.1.1.6 are available for download, Trellix recommends you download version 10.1.1.6. The latest version of software always contains the changes included in all previous releases. If necessary, you can also downgrade your Sensor by choosing from the list of available versions.

#### Note

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

#### Steps:

1. For a standalone Sensor, click Devices → <Admin Domain Name> → Devices → <Device Name> → Maintenance → Deploy Device Software. For Sensors in a stack, select Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → 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.

#### Note

<Device Name> refers to name of the Sensor.

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

### Note

The Software Ready for Installation section lists the applicable versions of software that you downloaded from the update server. (Manager → <Admin Domain Name> → Trellix IPS Protection Status. Select Device Software tab. The Device Software tab is displayed. Then, select Download Device Software option.)

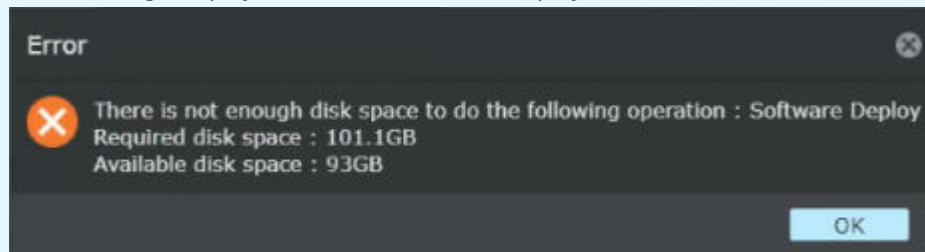
3. Click Upgrade. When a device is being updated, it continues to function using the software that was present earlier.

### Note

The Manager reserves 100 GB under required free disk space for Manager operations and considers an additional file size of 1.2 GB to be generated for each software deployment request. Upon receiving the request (single or in bulk), it checks the number of Sensors selected, and calculates the free disk space. If there is insufficient free disk space, an error message is displayed in the UI stating the available disk space and the space required to complete the upgrade task. This enables the Manager to reserve sufficient disk space to keep other processes running and avoid any software upgrade failure scenario.

---

Error message displayed for device software deployment if there is insufficient disk space



4. After the update is complete, restart the Sensor. If the device that you updated is a Sensor in a fail-over pair, 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

The Shut Down action turns off a Sensor with no restart.

1. For a standalone Sensor, select Devices → <Admin Domain Name> → Devices → <Device Name> → Maintenance → Shut Down. For Sensors in a stack, select Devices → <Admin Domain Name> → <Device Name> → Member Sensors → <Stackname-node id> → Maintenance → Shut Down. The Shut Down page is displayed.

2. Click Shut Down Now.

### Note

The <Device Name> could be a Sensor.

:

## 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 to your Manager server. The diagnostics file includes debug, log, and other information that can be used to determine device malfunctions or other performance issues. Once uploaded to your Manager, this file can be sent through email to Trellix Technical Support for analysis and troubleshooting advice.

### Steps:

1. For a standalone Sensor, select Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → Diagnostics Trace. For Sensors in a stack, select Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Troubleshooting → Diagnostics Trace.

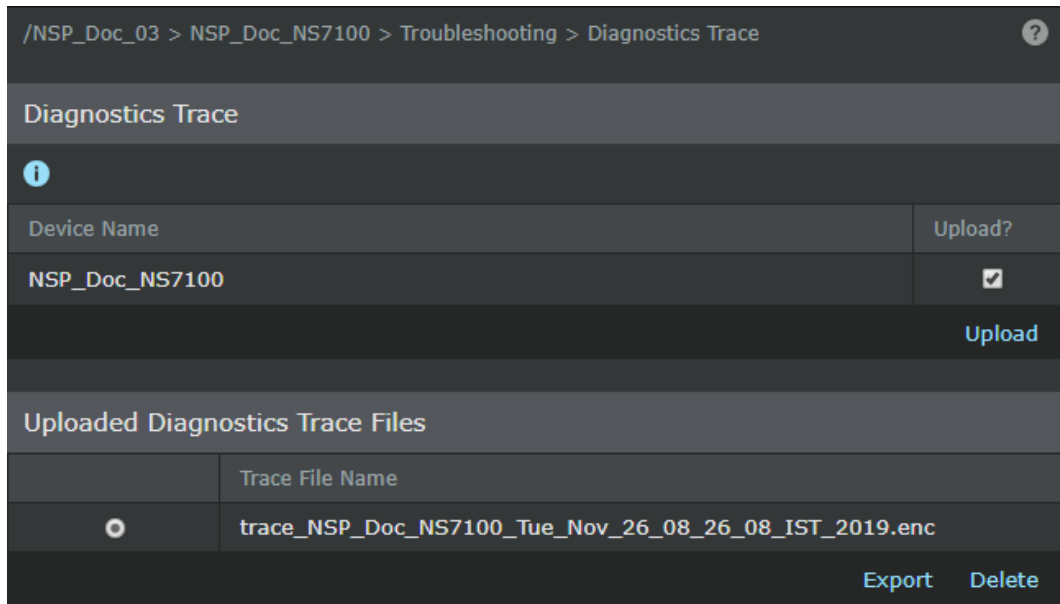
### Note

The <Device Name> refers to a Sensor.

The Diagnostics Trace page is displayed.

---

Diagnostics Trace page



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:

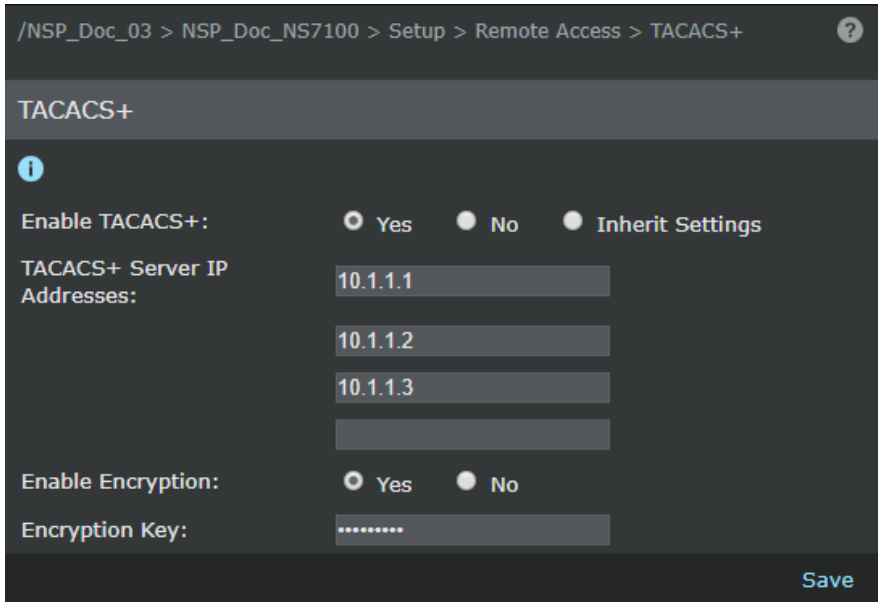
- Configure TACACS+ authentication
- Configure NMS objects

:

### Configure TACACS+ authentication

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

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.

### NMS Users sub-tab

Name	Created in Domain
TestUser	Sensor
NSPDocTest	Sensor

### Note

Only 10 users can be allocated or added onto the device.

:

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

### Steps:

1. Select Devices → <Admin Domain Name> → Devices → <Device\_Name> → Setup → Remote Access → NMS → NMS Users.
2. Click Assign Domain User.

### Note

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.

:

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

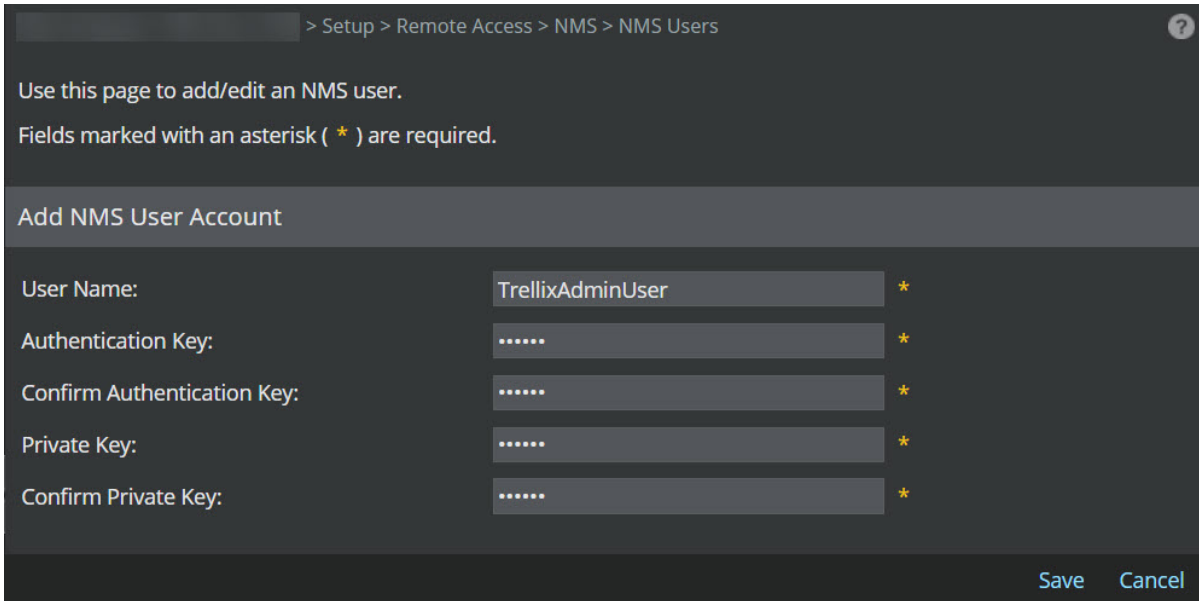
### Steps:

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 .

### Add NMS User Account dialog



> Setup > Remote Access > NMS > NMS Users

Use this page to add/edit an NMS user.  
Fields marked with an asterisk ( \* ) are required.

Add NMS User Account

User Name: TrellixAdminUser \*

Authentication Key: \*\*\*\*\* \*

Confirm Authentication Key: \*\*\*\*\* \*

Private Key: \*\*\*\*\* \*

Confirm Private Key: \*\*\*\*\* \*

Save Cancel

The Add NMS User Account dialog is displayed.

3. Enter the User Name.

### Note

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).

### Note

The length of the Authentication and Private key should be between 8 to 15 characters.



### Note

Since the communication is over SNMP version 3, the supported authentication protocol is "SHA1" and encryption algorithm is "AES128".

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

:


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

#### Steps:

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.

### Note


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 .
4. Enter the Authentication Key and Private Key (confirm at Confirm Authentication Key and Private Key).
5. Click Save; click Cancel to abort.

:

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

#### Steps:

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 .
4. Confirm deletion by clicking OK.

### Note

If an allocated user (user created at domain) is deleted, it is deleted only at the device settings level and not from the domain.

:

## 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.

### Note

NMS will not work for default port 161 of NS-series Sensors.

:

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

### Steps:

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.

:

NMS IP addresses can be added from the device and from the domain.

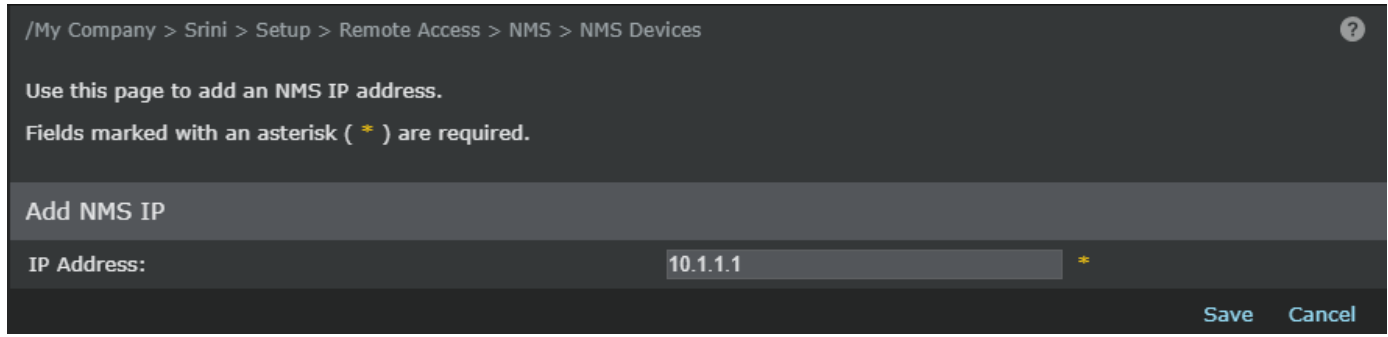
### Steps:

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 .

---

Add NMS IP dialog



/My Company > Srimi > Setup > Remote Access > NMS > NMS Devices

Use this page to add an NMS IP address.  
Fields marked with an asterisk ( \* ) are required.

### Add NMS IP

IP Address:  \*

Save Cancel

The Add NMS IP page is displayed.

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

#### Note


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

4. Click Save.

:

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

#### Steps:

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 .
4. Confirm deletion by clicking OK.

#### Note

If allocated IP addresses are deleted, those are deleted only from the device and not from the domain.

 **Note**

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, the connection from that IP address remains 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 Update Server. These updates include signature files for your Sensors and software for your Manager and/or Sensors.

 **Note**

You can only perform one download/upload at a time from any Trellix IPS 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 *Trellix Intrusion Prevention System Product Guide*.

:

## Uninstallation of the Manager/Central Manager

You uninstall the Manager and the Central Manager using the standard Windows Add/Remove Programs feature.

 **Note**

Uninstallation of the Manager/Central Manager is not supported in Linux based Manager/Central Manager.

:

### Uninstall using the Add/Remove program

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

To uninstall the Manager software:

### Note

Trellix 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 IPS Manager program folder.

### Steps:

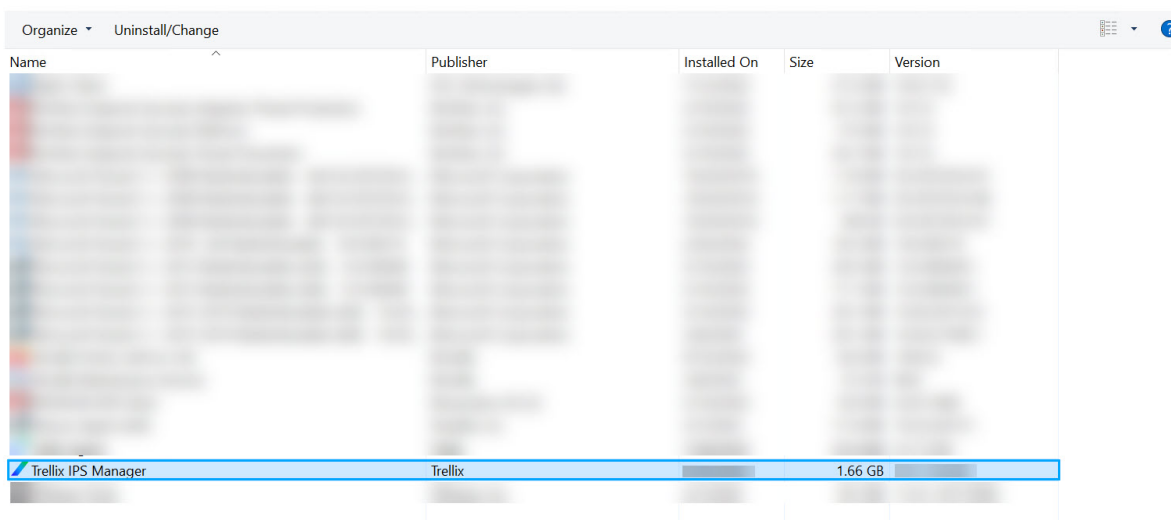
1. Go to Start → Settings → Control Panel → Add/Remove Programs and select Trellix IPS Manager.

---

#### Programs and Features in Control Panel

[Uninstall or change a program](#)

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

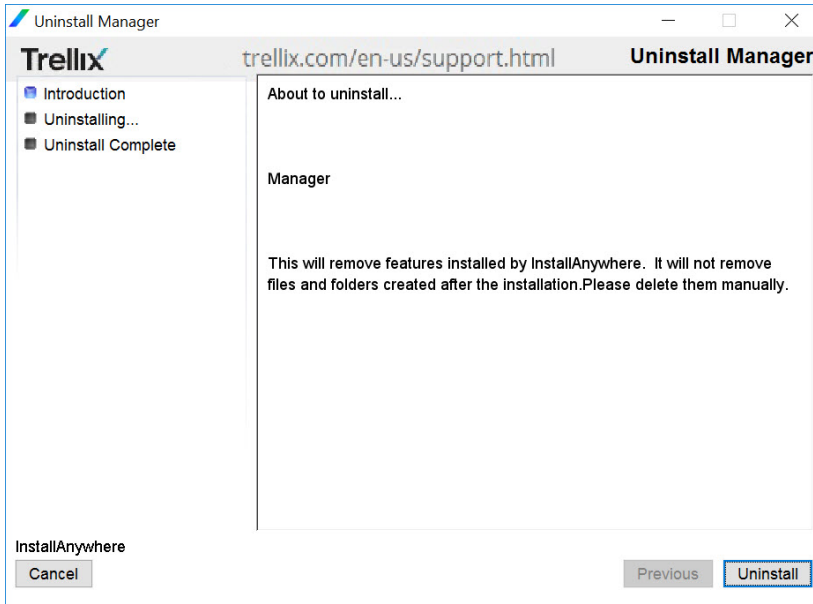


The Uninstall Manager window appears.

2. Click Uninstall to start the uninstallation process.

---

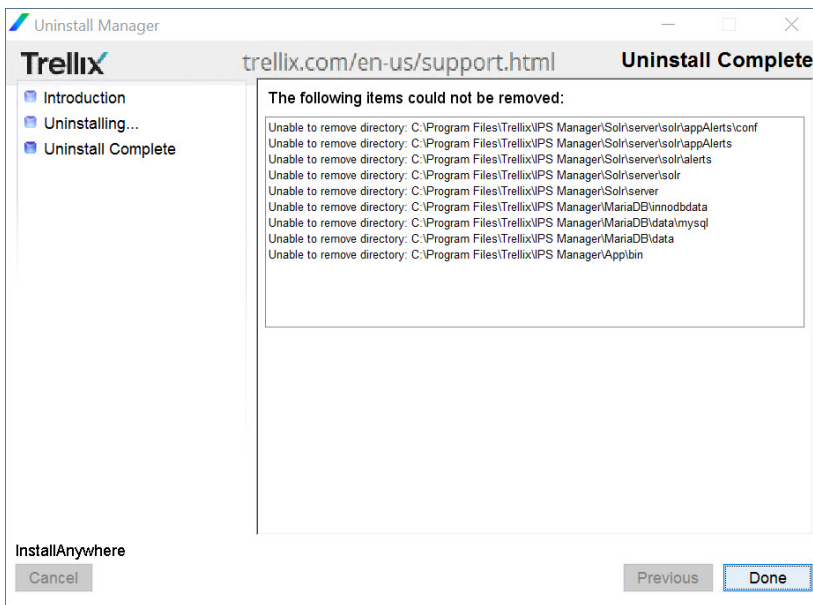
#### Uninstall Manager window



3. After uninstallation, the message The following items could not be removed: is displayed along with a list of directories that were not removed during uninstallation. Click Done.

---

Uninstall Complete window



### Note

Log files, archival files, databases (MariaDB and Solr) and user specific data are not removed during the uninstallation. This data still remains in the Manager install directory. If you wish to remove all this data, navigate to the location where you installed the Manager and delete the IPS Manager directory.

:

### Uninstall using the script

You can also uninstall the Windows based Manager/Central Manager by executing a script from the IPS Manager program folder.

To uninstall via script:

#### Steps:

1. Navigate to the directory containing the uninstallation script. The default path is: <Manager\_Install\_Dir> \App\UninstallerData
2. Run **Uninstall\_ems.exe**The Uninstall Manager window appears. Later, follow the same steps as mentioned in **Step 2** of **Uninstall using the Add/Remove program** section.

:

# Upgrading Trellix Intrusion Prevention System

This section of the guide primarily provides information on how to upgrade your Trellix IPS setup to the latest 11.1 release from 10.1 version.

:

## Overview

### Important Notes:

- The Manager software version 10.1.7.50 and above supports only TLS 1.2 ciphers for Manager and Sensor communication.

### Caution

If you are currently using Sensor software version that supports TLS 1.0 and you upgrade your Manager to any software version that supports only TLS 1.2, the communication between the Manager and Sensor will fail. Therefore, you must first upgrade the Sensor to a software version that supports TLS 1.2 and later upgrade your Manager to the desired version. Post this, you may upgrade the Sensor to any later version as per your requirement. Refer to [KB96194](#) for more information.

- The Trellix IPS 11.1 release is applicable to the Central Manager, Manager, NS-series Sensors and Virtual IPS Sensors.
- As with any upgrade, Trellix strongly recommends that you always first try the upgrade in a test environment.
- The current version of 11.1 Manager software can be used to configure and manage the following:
  - NS-series Sensors on 10.1, and 11.1 software
  - Virtual IPS Sensors on 10.1, and 11.1 software
  - NTBA Appliances (physical and virtual) on 9.1 software
- The upgrade involves the following phases that you must complete in the same order:
  - If applicable, Trellix IPS Central Manager upgrade.
  - Trellix IPS Manager upgrade.
  - NS-series Sensor software or Virtual IPS Sensor software upgrade.

### Important

You must disconnect any M-series Sensors configured in the 10.1 Manager before upgrading to 11.1 Manager.

You will require the *Trellix Intrusion Prevention System 11.1 Product Guide* during the upgrade process.



It is also strongly recommended that you read the Release Notes for the associated product before you upgrade because this document makes references to several new features and enhancements.

:

### Important requirements and considerations

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

- This document provides information on how to upgrade from Trellix Intrusion Prevention System version 10.1 to Trellix Intrusion Prevention System version 11.1. See the corresponding upgrade section and release notes to first upgrade to the minimum required version for 11.1, if you are on a version other than the ones mentioned here. Consider that your current version is in the 9.1 or 9.2 release train but your current version is not supported for upgrade to 11.1. You need to upgrade your deployments to a compatible 10.1 version before you upgrade to 11.1. Refer to *Release Information* section in the following release notes to upgrade your existing 9.x deployments to 10.1. Post this, you can upgrade your deployments to 11.1: [IPS 10.1.7.65-10.1.5.190 NS-Series Release Notes](#) [VIPS 10.1.7.65-10.1.7.155 Virtual IPS Release Notes](#)
- For 9.1 or 9.2 version software images, contact Trellix Technical Support.
- The minimum required software versions to upgrade to 11.1 are provided in the following sections:
  - [Upgrade path for the Central Manager and Manager.](#)
  - [Sensor upgrade requirements.](#)
- After you upgrade the Linux based Central Manager or the Manager to 11.1, you will be prompted to restart the server.
- Following are the ports that are used for Sensor-to-Manager communication in release 11.1. Before you begin the 11.1 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). For the list of ports to be opened, refer to the section *Set the desktop firewall* in *Trellix Intrusion Prevention System Product Guide*.

:

## Management of a heterogeneous environment

Trellix IPS 11.1 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](#).

:

### 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 11.1.7.x, the major version is 11.1. For Manager 10.1.7.x, the major version is 10.1.

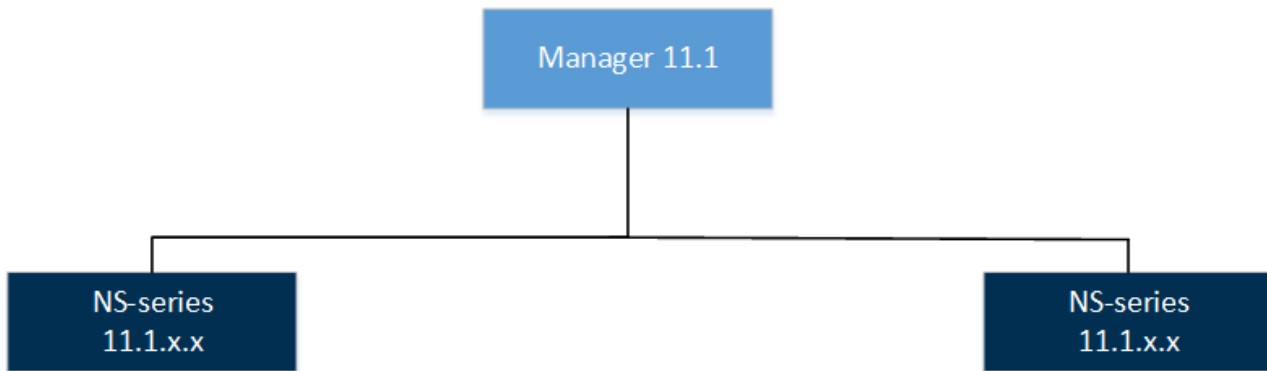
If the Manager and the Sensors are of the same major version, it is referred to as a homogeneous environment. In a heterogeneous environment, the Manager and the Sensors are of different successive major versions. This applies to the Central Manager and the Managers as well.

### Note

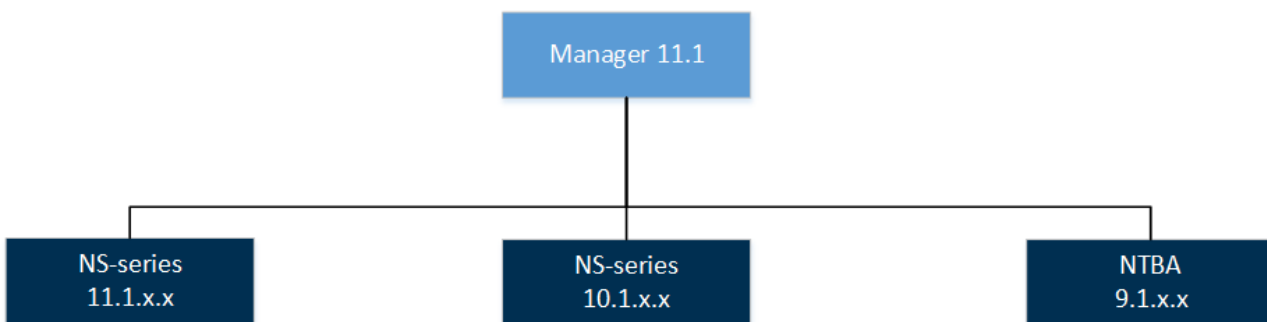
The terms heterogeneous and homogeneous environments are used with respect to the software versions only and have no relevance to the device model numbers.

---

Homogeneous environment - an example



Heterogeneous environment - an example



Notes:

- A Manager must always be of the same or higher version than the corresponding Sensors. Therefore, a 10.1 Manager managing 11.1 Sensors is not a valid scenario. Similarly, the Central Manager must be of the same or higher version than the corresponding Managers.
- The latest 11.1 Manager can manage only the NS-series, Virtual IPS, and NTBA devices on the following software versions — 11.1.x.x and 10.1.x.x (for Sensors) and 9.1.x.x (for NTBA). Similarly, a 11.1 Central Manager can manage 10.1.x.x and 11.1.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.

:

### 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 10.1.x.x. As part of the upgrade process, you first upgrade the Manager as well as some of the Sensors to 11.1. However, during this upgrade window, you might need to manage the 10.1 Sensors as well as be able to view the alerts raised by them. For any reason, if you do have the latest version of the Sensor software but need to manage such Sensors as well, this is possible with a Manager version that supports a heterogeneous Sensor environment.

Trellix 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 Trellix IPS.

:

### 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 NS-series Sensors, a 11.1 Manager can manage the NTBA devices as well.
- 11.1 device software is available only for NS-series and Virtual IPS Sensors.

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 [Scenarios involving the Manager](#).

- Upgrade from a homogeneous 10.1 Manager environment to a heterogeneous 11.1 Manager environment:
  - [Scenario 1: Standalone setup](#)
  - [Scenario 2: MDR setup](#)
- Upgrade from a heterogeneous 10.1 Manager environment to a heterogeneous 11.1 Manager environment:
  - [Scenario 3: Standalone setup](#)
  - [Scenario 4: MDR setup](#)

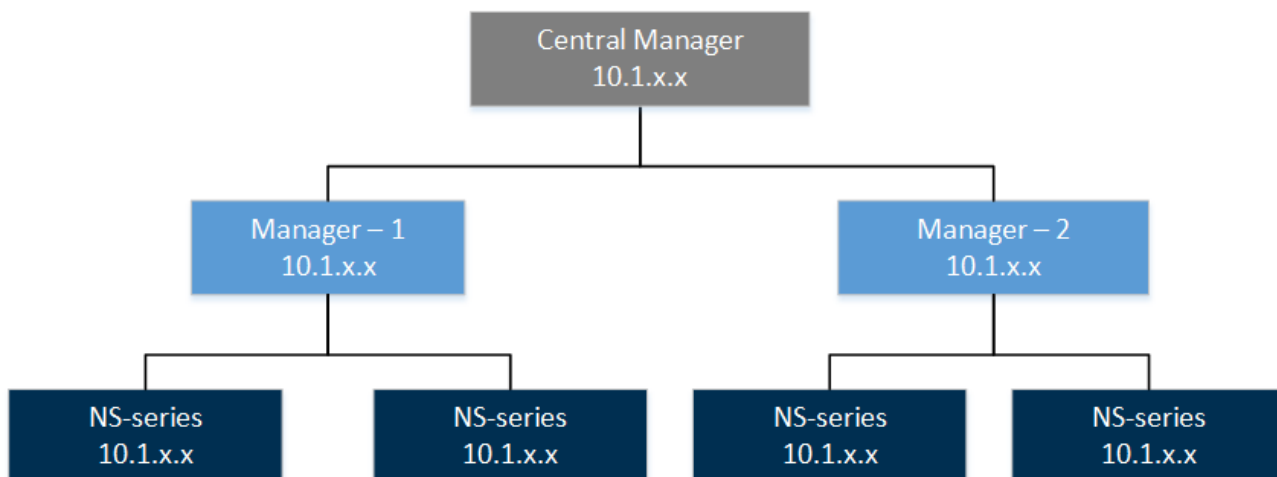
### Note

Review [Minimum required Central Manager version](#) to know the version of the Central Manager that you need to upgrade to 11.1.

:

### Scenario 1 – Homogeneous, standalone setup

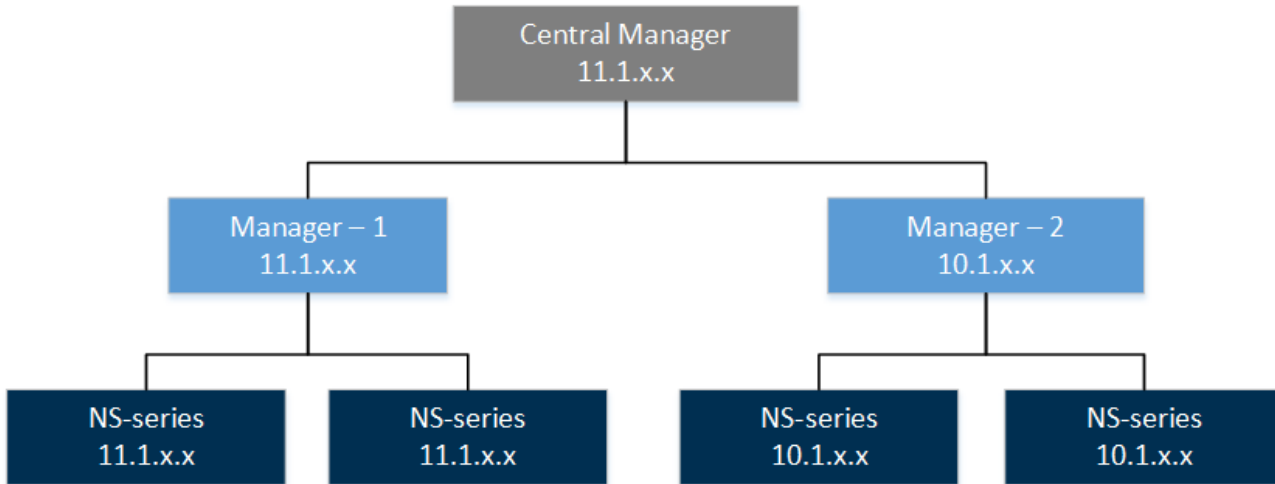
This scenario is about an upgrade from a homogeneous Manager environment to a heterogeneous 11.1 Manager environment managed by a standalone Central Manager.



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 11.1 version. If not, make sure you upgrade them to the required versions before you begin your 11.1 version.
2. Make sure your current Trellix IPS deployment is functioning as configured and without any issues.

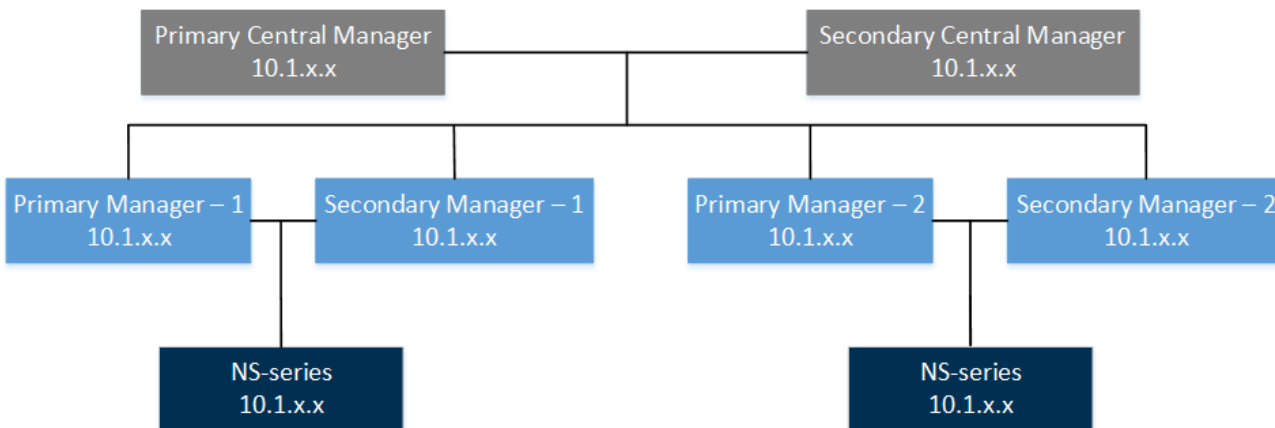
3. Upgrade the standalone Central Manager to the latest 11.1 version. See [Upgrading the Central Manager](#).
4. Upgrade the required Managers to the latest 11.1 version. See [Upgrading the Manager](#).
5. Upgrade the required Sensors managed by the 11.1 Managers. See [Performing Signature Set and Sensor Software upgrade](#).



:

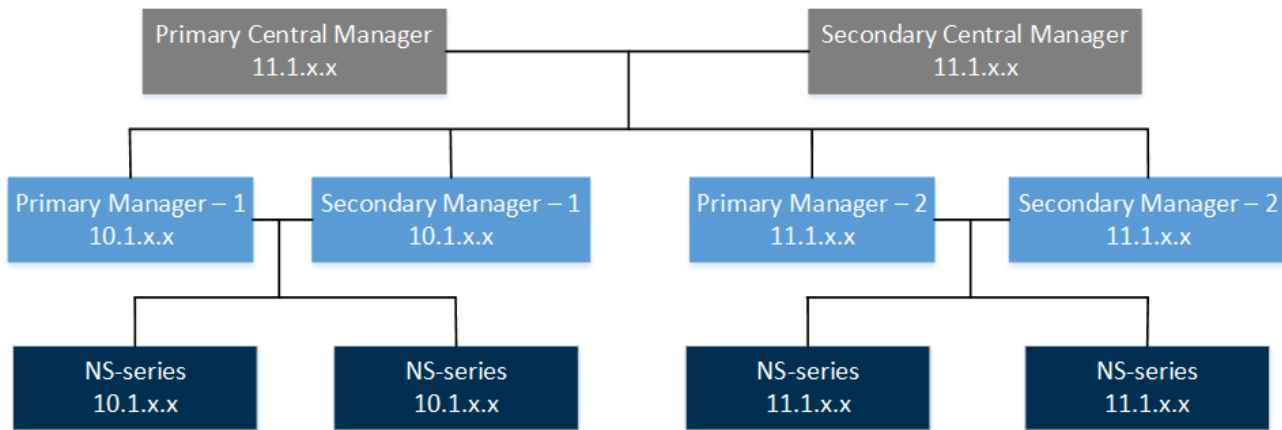
### Scenario 2 – Homogeneous, MDR setup

This scenario is about an upgrade from a homogeneous Manager environment to a heterogeneous 11.1 Manager environment managed by an Manager Disaster Recovery (MDR) pair of Central Managers.



The upgrade path for this scenario is as follows:

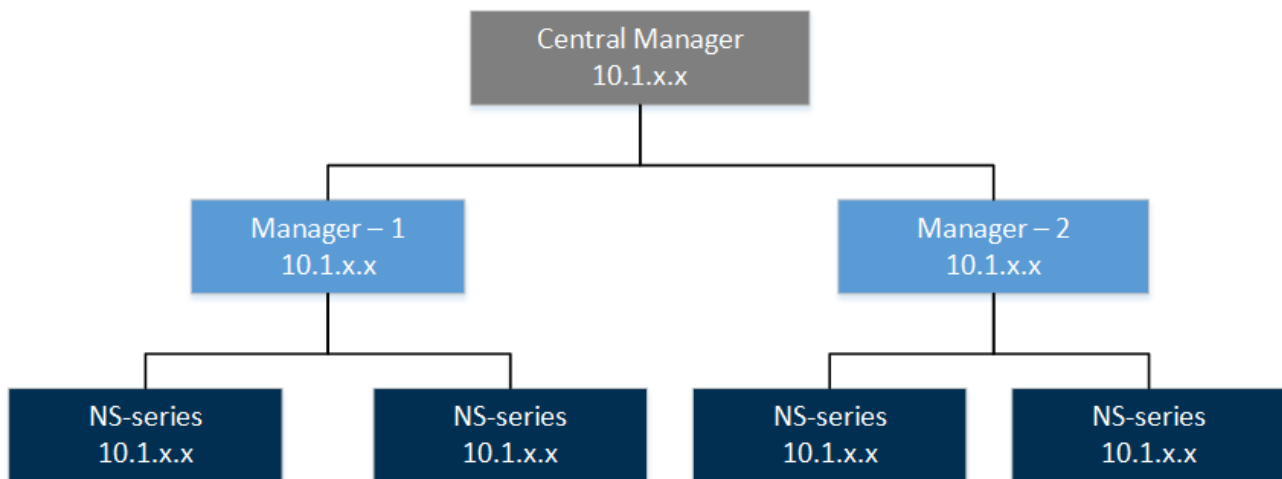
1. Make sure the Central Managers, Managers, and Sensors meet the minimum required versions to upgrade to the latest 11.1 version. If not, make sure you upgrade them to the required versions before you begin your 11.1 version.
2. Make sure your current Trellix IPS deployment is functioning as configured and without any issues.
3. Upgrade the Central Manager MDR pair to the latest 11.1 version. See [Upgrading the Central Manager](#).
4. Upgrade the required Manager MDR pairs to the latest 11.1 version. See [Upgrading the Manager](#).
5. Upgrade the required Sensors to the latest 11.1 version. See [Performing Signature Set and Sensor Software upgrade](#).



:

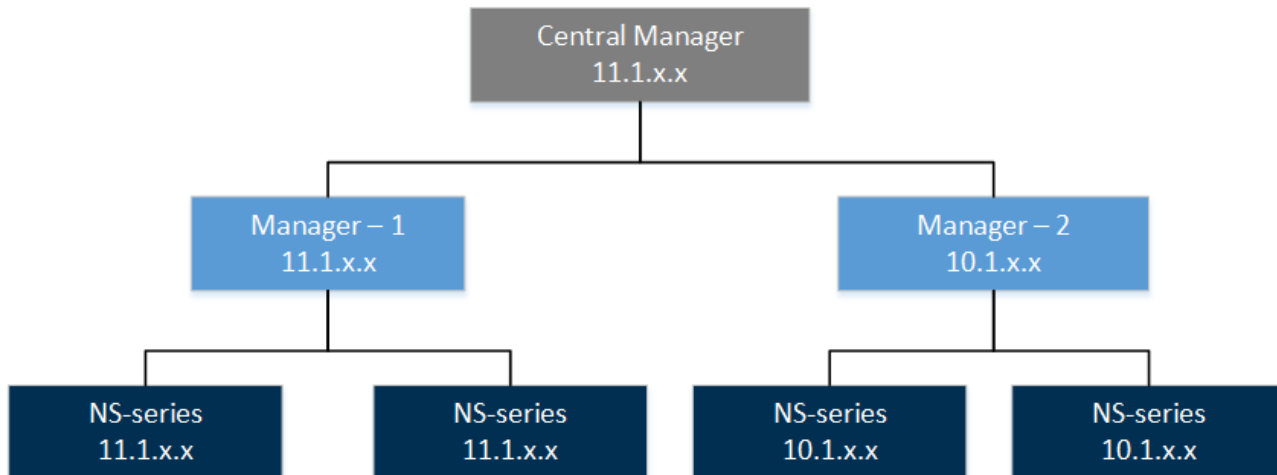
### Scenario 3 - Heterogeneous, standalone setup

This scenario is about an upgrade from a heterogeneous Manager environment to a heterogeneous Manager environment in 11.1, managed by a standalone Central Manager.



The upgrade path for this scenario is as follows:

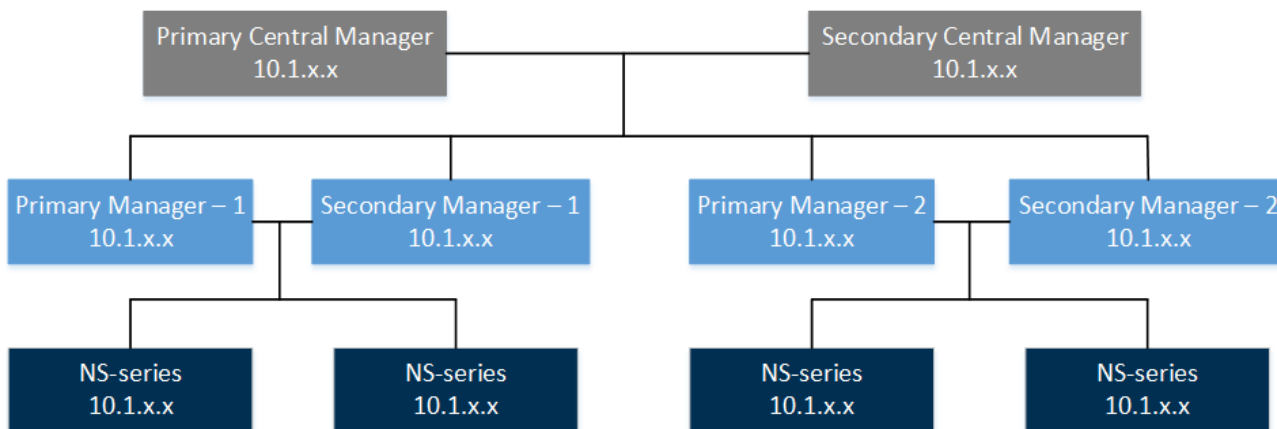
1. Make sure the Central Manager, Managers, and Sensors meet the minimum required versions to upgrade to the latest 11.1 version. If not, make sure you upgrade them to the required versions before you begin your 11.1 version.
2. Make sure your current Trellix IPS deployment is functioning as configured and without any issues.
3. Upgrade the standalone Central Manager to the latest 11.1 version. See [Upgrading the Central Manager](#).
4. Upgrade the required Managers to the latest 11.1 version. See [Upgrading the Manager](#).
5. Upgrade the required Sensors to the latest 11.1 version. See [Performing Signature Set and Sensor Software upgrade](#).



:

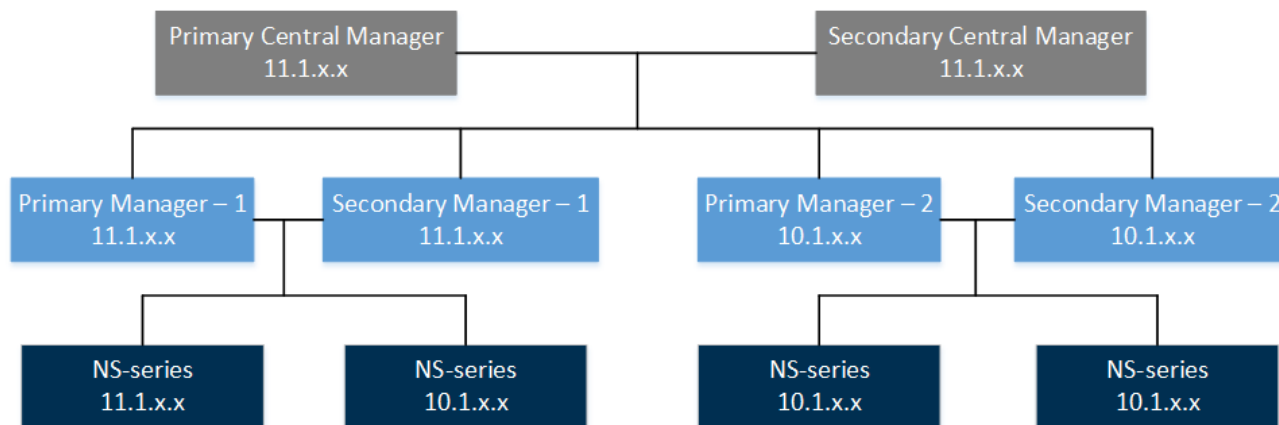
### Scenario 4 - Heterogeneous, MDR setup

This scenario is about an upgrade from a heterogeneous Manager environment to a heterogeneous 11.1 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 11.1 version. If not, make sure you upgrade them to the required versions before you begin your 11.1 version.
2. Make sure your current Trellix IPS deployment is functioning as configured and without any issues.
3. Upgrade the Central Manager MDR pair to the latest 11.1 version. See [Upgrading the Central Manager](#).
4. Upgrade the required Manager MDR pairs to the latest 11.1 version. See [Upgrading the Manager](#).
5. Upgrade the required Sensors to the latest 11.1 version. See [Performing Signature Set and Sensor Software upgrade](#).



:

### Manager upgrade scenarios

The following scenarios involve the Manager:

- Upgrade from a homogeneous Sensor environment in 10.1 to a heterogeneous Sensor environment in 11.1:
  - [Scenario 5: Standalone Manager setup](#)
  - [Scenario 6: MDR setup](#)
- Upgrade from a heterogeneous Sensor environment in 10.1 to a heterogeneous Sensor environment in 11.1:
  - [Scenario 7: Standalone Manager setup](#)
  - [Scenario 8: MDR setup](#)

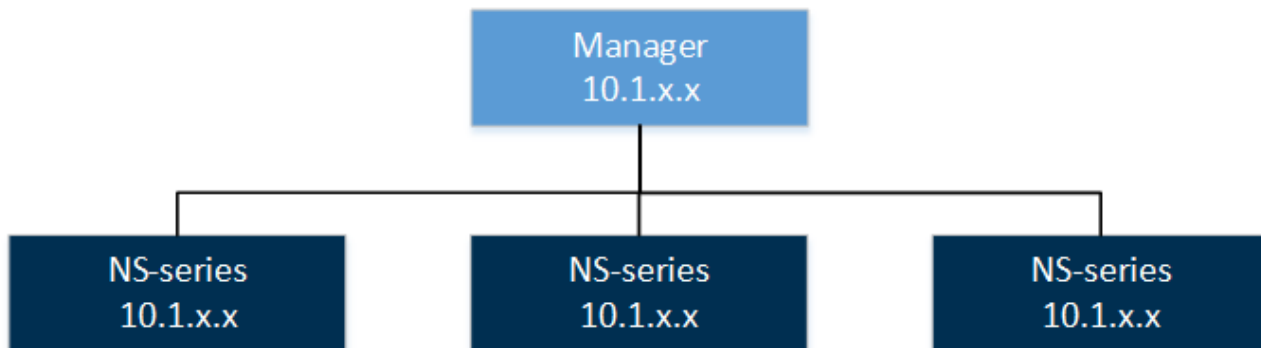
See [Upgrade path for the Central Manager and Manager](#) to know the Manager versions that you need to upgrade to the latest 11.1.

:

### [Scenario 5 - Homogeneous, standalone setup](#)

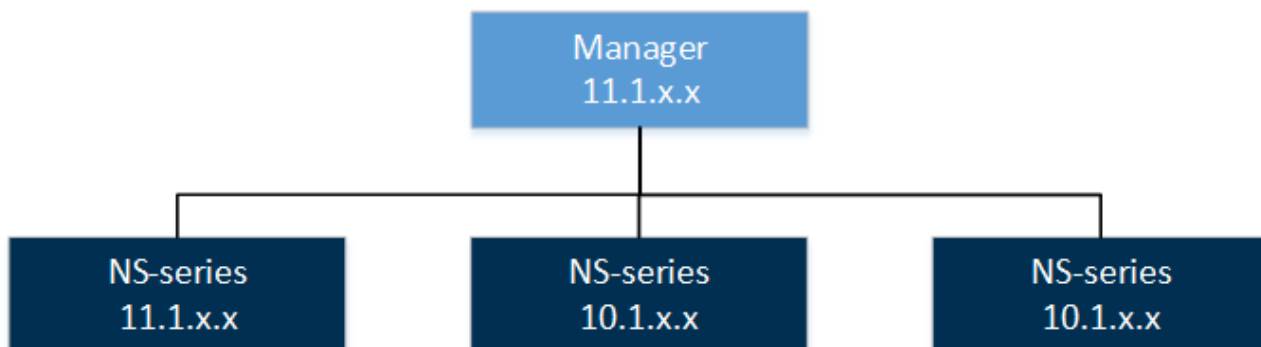


This scenario is about an upgrade from a homogeneous Sensor environment to a heterogeneous Sensor environment in 11.1, managed by a standalone Manager.



The upgrade path for this scenario is as follows:

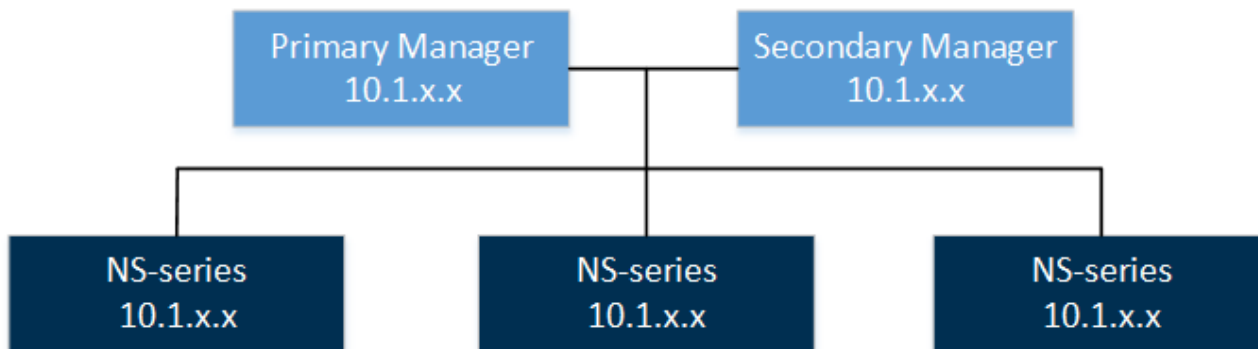
1. Make sure the Manager and Sensors meet the minimum required versions to upgrade to the latest 11.1 version. If not, make sure you upgrade them to the required versions before you begin your 11.1 version.
2. Make sure your current Trellix IPS deployment is functioning as configured and without any issues.
3. Upgrade the standalone Manager to the latest 11.1 version. See [Upgrading the Manager](#).
4. Upgrade the required Sensors to the relevant 11.1 version. See [Performing Signature Set and Sensor Software upgrade](#).



:

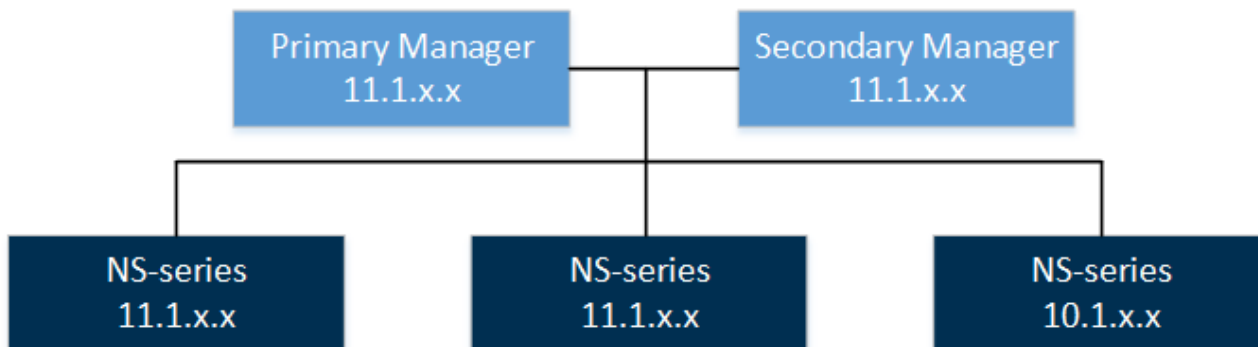
### Scenario 6 - Homogeneous, MDR setup

This scenario is about an upgrade from a homogeneous Sensor environment to a heterogeneous Sensor environment in 11.1, managed by an MDR pair of Managers.



The upgrade path for this scenario is as follows:

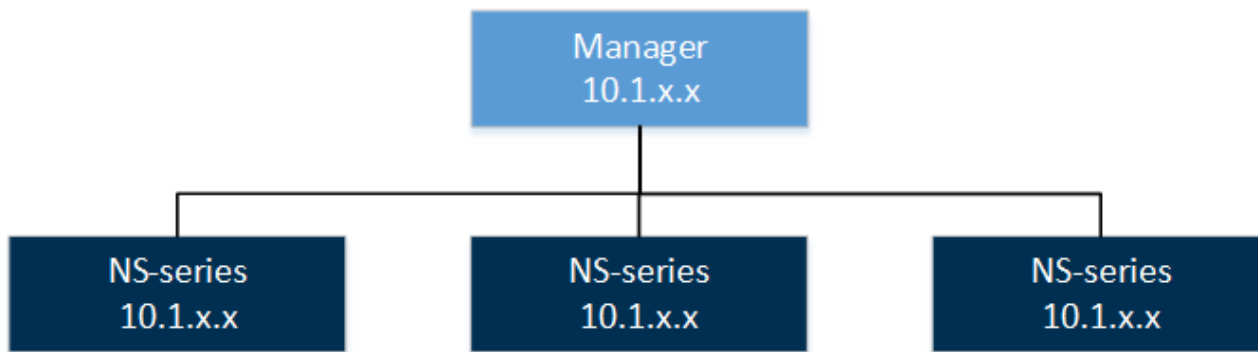
1. Make sure that Managers and Sensors meet the minimum required versions to upgrade to the latest 11.1 version. If not, make sure that you upgrade them to the required versions before you begin your 11.1 version.
2. Make sure your current Trellix IPS deployment is functioning as configured and without any issues.
3. Upgrade the Manager MDR pair to the latest 11.1 version. See [Upgrading the Manager](#).
4. Upgrade the required Sensors to the latest 11.1 version. See [Performing Signature Set and Sensor Software upgrade](#).



:

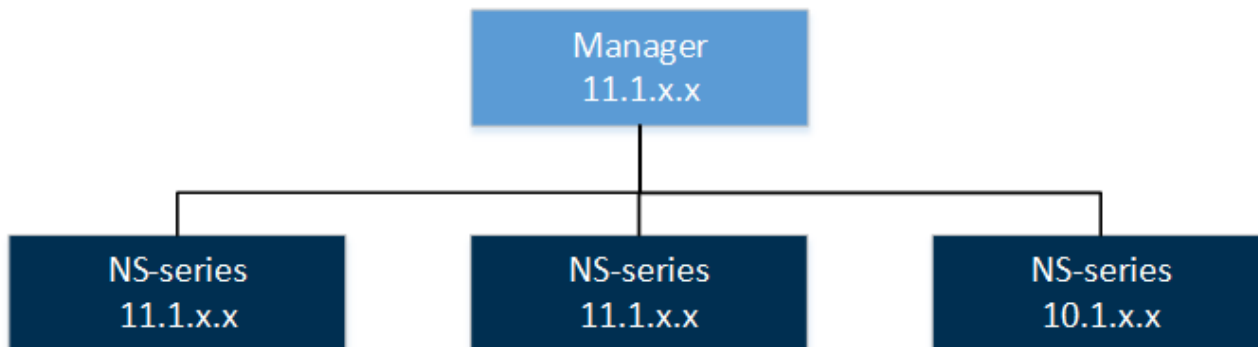
### Scenario 7 - Heterogeneous, standalone setup

This section describes the upgrade for a heterogeneous Sensor environment managed by a standalone Manager.



The upgrade path for this scenario is as follows:

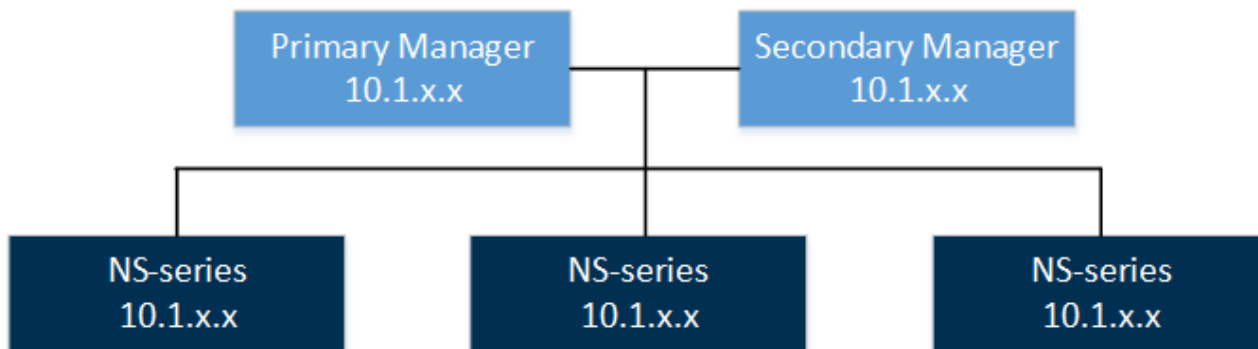
1. Make sure the Manager and Sensors meet the minimum required versions to upgrade to the latest 11.1 version. If not, make sure you upgrade them to the required versions before you begin your 11.1 version.
2. Make sure your current Trellix IPS deployment is functioning as configured and without any issues.
3. Upgrade the standalone Manager to the latest 11.1 version. See [Upgrading the Manager](#).
4. Upgrade the required Sensors to the latest 11.1 version. See [Performing Signature Set and Sensor Software upgrade](#).



:

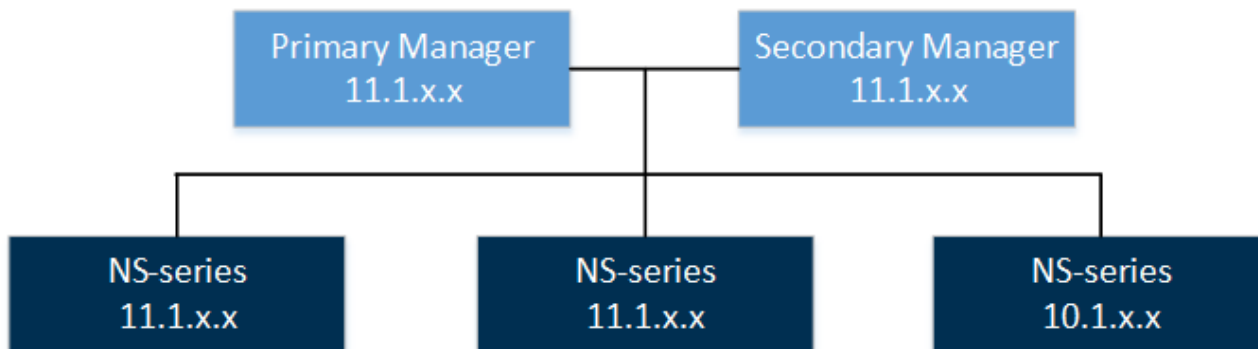
### Scenario 8 – Heterogeneous MDR

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 11.1 version. If not, make sure you upgrade them to the required versions before you begin your 11.1 version.
2. Make sure your current Trellix IPS deployment is functioning as configured and without any issues.
3. Upgrade the Manager MDR pair to the latest 11.1 version. See [Upgrading the Manager](#).
4. Upgrade the required Sensors to the latest 11.1 version. See [Performing Signature Set and Sensor Software upgrade](#).



:

### Heterogeneous support for NTBA devices

You can manage a heterogeneous NTBA environment using Manager 11.1.

#### Note

Software version 10.1 and 11.1 for NTBA Appliance is not available.

#### 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 9.1 NTBA device managed by Manager 11.1.

Supported heterogeneous combinations

Manager version	Sensor version	Supported NTBA versions
11.1	10.1	9.1
	11.1	9.1

:

## How to upgrade the Central Manager?

If you have the Central Manager deployed, you must upgrade it to 11.1 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 11.1. If you have not deployed a Central Manager, proceed to [How to Upgrade the Manager?](#).

:

### Upgrade requirements for the Central Manager

This chapter discusses the requirements for a successful upgrade of the Central Manager.

:

### Upgrade path for the Central Manager

A direct upgrade to Central Manager or Manager 11.1 from versions earlier than what is mentioned in this section is not supported.

#### Upgrade paths for Windows based Manager software versions

Required Central Manager/Manager versions

Version	Upgrade path to 11.1
10.1.7.4, 10.1.7.7, 10.1.7.29, 10.1.7.35, 10.1.7.40, 10.1.7.44, 10.1.7.50, 10.1.7.50.2, 10.1.7.55, 10.1.7.61, 10.1.7.65, 10.1.7.66.3, 10.1.7.66.11	11.1.7.71
11.1.7.3, 11.1.7.3.5, 11.1.7.26, 11.1.7.41, 11.1.7.41.2, 11.1.7.56	11.1.7.71

### Important

If you are using a hotfix release, contact Trellix support for the recommended upgrade path.

### Upgrade paths for Linux based Manager software versions

### Caution

After upgrade, the Linux-based Manager reboot automatically. If it fails to reboot, check the installation logs for errors and reboot the Manager manually.

Version	Upgrade path to 11.1
10.1.7.4, 10.1.7.7, 10.1.7.25 (Cloud), 10.1.7.29, 10.1.7.35, 10.1.7.40, 10.1.7.44, 10.1.7.50, 10.1.7.50.2, 10.1.7.55, 10.1.7.61, 10.1.7.65, 10.1.7.66 (Cloud), 10.1.7.66.3, 10.1.7.66.11	11.1.7.71
11.1.7.3, 11.1.7.3.5, 11.1.7.26, 11.1.7.41, 11.1.7.41.2, 11.1.7.56	11.1.7.71

### Note

For all direct upgrades to 11.1.7.71, use the **IPSM\_111771\_setup.bin Version 11.1.7.71** upgrade file.

 **Important**

If you are using a hotfix release, contact Trellix support for the recommended upgrade path.

:

## Considerations for Linux based Central Manager/Manager

Make sure to review all considerations mentioned in this section before you proceed with Linux based Manager installation or upgrade :

- In a Linux based MDR pair, both Primary and Secondary Managers should be Linux based. For example, you cannot create an MDR pair, if your Primary Manager is Windows based and Secondary Manager is Linux based or vice versa.
- The Linux based Central Manager can only manage the Linux based Managers.
- The Linux based Central Manager must be of the same or a higher version than the corresponding Linux based Managers.

:

## 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.

 **Note**


These suggestions do not take into account the amount of disk space you require for alert and packet log storage. See the *Trellix Intrusion Prevention System Product Guide* for suggestions on calculating your database capacity requirements.

The following table lists the 11.1 Windows based Manager/Central Manager application requirements:



 **Note**

Windows Server 2012 Standard/Windows Server 2012 R2 Standard is not supported for the Manager.

	<b>Minimum required</b>	<b>Recommended</b>
Operating system	Any of the following: <ul style="list-style-type: none"><li>• Windows Server 2016 Standard Edition English operating system</li></ul>	Windows Server 2022 Datacenter Edition operating system

	Minimum required	Recommended
	<ul style="list-style-type: none"> <li>• Windows Server 2016 Standard Edition Japanese operating system</li> <li>• Windows Server 2016 Datacenter Edition English operating system</li> <li>• Windows Server 2016 Datacenter Edition Japanese operating system</li> <li>• Windows Server 2019 Standard Edition English operating system</li> <li>• Windows Server 2019 Standard Edition Japanese operating system</li> <li>• Windows Server 2019 Datacenter Edition English operating system</li> <li>• Windows Server 2019 Datacenter Edition Japanese operating system</li> <li>• Windows Server 2022 Standard Edition English operating system</li> <li>• Windows Server 2022 Standard Edition Japanese operating system</li> <li>• Windows Server 2022 Datacenter Edition English operating system</li> <li>• Windows Server 2022 Datacenter Edition Japanese operating system</li> </ul> <div style="background-color: #e0f2f7; padding: 5px; margin-top: 10px;"> <p> <b>Note:</b> Only x64 architecture is supported.</p> </div>	



	Minimum required	Recommended
Memory	16 GB  <b>Note:</b> Supports up to 10 million alerts in Solr	>=32 GB  <b>Note:</b> Supports up to 20 million alerts in Solr
CPU	Server model processor, such as Intel Xeon	Same
Disk space	300 GB	500 GB or more
Network	1 Gbps card	1 Gbps card
Virtual CPUs (Applicable only on a VMware platform)	4	4 or more

 **Note**


You need Windows Administrator permission for the server machine.

 **Tip**

The *Trellix Intrusion Prevention System Product Guide* provides a number of pre-installation tips and suggestions with which Trellix recommends you to 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 table lists the 11.1 Linux based Manager/Central Manager application specifications for an OVA file:

Component	Specifications
MLOS	3.9.1
Logical CPU cores	8

Component	Specifications
Memory	32 GB
Disk space	500 GB
NIC	1  <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;">  <b>Note:</b>                      You can consider 2 for a dual NIC configuration.                 </div>

### How to host the Manager on a VMware platform


#### VMware ESXi server requirements for Windows Operating System

Component	Supported
Virtualization software	<ul style="list-style-type: none"> <li>ESXi 7.0 Update 3</li> <li>ESXi 8.0</li> </ul> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;">  <b>Note:</b>                      Hyperthreading should be available.                 </div>

The following are the system requirements for hosting 11.1 Linux based Manager/Central Manager application on a VMware platform:

#### VMware ESXi server requirements for MLOS

Component	Supported
Virtualization software	<ul style="list-style-type: none"> <li>ESXi 7.0 Update 3</li> <li>ESXi 8.0</li> </ul>

Component	Supported
	 <b>Note:</b> Hyperthreading should be available.

### How to host the Manager on KVM

The following table lists the 11.1 Linux based Manager/Central Manager application specifications for a qcow2 file:

Component	Specifications
MLOS	3.9.1
Logical CPU cores	8
Memory	20 GB
Disk space	500 GB
NIC	1

The following are the system requirements for hosting 11.1 Linux based Manager/Central Manager application on KVM:

KVM server requirements for MLOS

Component	Supported
Virtualization software	KVM 2.12.0

:

### Preparation for the upgrade

After you make sure you meet the requirements, prepare for the upgrade.

#### Caution

Before you begin the upgrade, make sure that no processes related to Trellix IPS (such as automated database archival) are scheduled during the upgrade time frame. Any such concurrent activity might cause conflicts and result in upgrade failure.

Make sure to review all considerations mentioned in this section before you proceed with the upgrade.

:

### Backing up Trellix IPS data

Before you upgrade, back up your tables and save any Trellix IPS custom attacks 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.

#### Note

Save your entire backup in a different location than the current Central Manager or Manager to prevent data loss.

After you back up the Trellix IPS data, you can consider purging the Manager tables. Details on how to purge the database tables are in the *Trellix Intrusion Prevention System Product 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. Trellix 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, Trellix 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 *Trellix Intrusion Prevention System Product Guide*.

:

### Back up Trellix IPS custom attacks

If you have Trellix IPS custom attacks, back them up prior to upgrade. Refer to the corresponding version of the *Trellix Intrusion Prevention System Product Guide* for information on how to back up custom attacks from the Central Manager and Manager.

:

### Review the upgrade considerations

Review this section carefully before you commence the upgrade process of the Central Manager.

- **Central Manager upgrade downtime window** — How long the upgrade takes depends on the size of your deployment and the size of your database. The upgrade process of Central Manager itself may take an hour to complete.
  - **Operating system upgrade downtime** — The latest Central Manager 11.1 is supported on various Windows and Linux operating systems as mentioned in [Central Manager and Manager system requirements](#). If you want to upgrade the operating system of your Central Manager server, for example from Windows Server 2016 to Windows 2022, 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 the earlier version if you encounter any problem during the upgrade. Backing up immediately following the upgrade preserves your upgraded tables and provides a baseline of the 11.1 database that you upgraded to. Importantly, when you are backing up the database, there should not be any scheduled task running in the background.

#### Note

You cannot restore the database from a lower version of the Central Manager on a higher version of Central Manager.

:

### Notes for upgrading the Central Manager from 10.1 to 11.1

If you are upgrading the Central Manager from version 10.1 to version 11.1, read the following sections carefully.

#### MLOS upgrade

Starting with this release of 11.1, the IPS Manager uses MLOS version 3.9.1 that includes additional security against new vulnerabilities.

This release provides the following enhancements related to platforms, environments, or operating systems:

### Apache Solr upgrade

With this release the IPS Manager uses Apache Solr version 8.11.2 that includes additional security against new vulnerabilities.

### Apache Tomcat upgrade

Starting with this release of 11.1, the IPS Manager uses Tomcat version 9.0.68 that includes additional security against new vulnerabilities and bug fixes.

:

## Central Manager and operating system upgrade

If you are considering an operating system upgrade as part of the 11.1 Central Manager upgrade, review the methods discussed under [Operating system upgrade for Windows based Manager](#).

:

## Standalone Central Manager upgrade

Trellix recommends that you regularly monitor for maintenance releases and new versions of the Central Manager software. To know whether the new version of the Central Manager is applicable to Linux appliances, see the specific version of Trellix Intrusion Prevention System release notes. The Linux based Central Manager upgrade file contains Central Manager software upgrade file bundled with MLOS upgrade patch. On executing the Linux based Central Manager upgrade file, the MLOS and the Linux based Central Manager software are upgraded simultaneously.

### Prerequisites:

- Your current Trellix IPS infrastructure meets all the requirements discussed in [Reviewing the upgrade requirements](#).
- 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 [Reviewing the Upgrade Considerations](#).
- You have backed up your current Central Manager data. See [Backing up Trellix IPS data](#).
- You have the latest 11.1 Central Manager installable file at hand. You can download it from the Trellix Download Server. See [Download the Manager/Central Manager executable](#) for information.
- You have your Central Manager database 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 database. The Central Manager cannot upgrade the database if the database is actively communicating with another application.

### Important

If this is an upgrade of a Central Manager in an MDR pair, switch the primary Central Manager to standby mode before you proceed. Make sure you are following the steps in [MDR Central Manager upgrade](#).

#### Steps:

1. Stop the Trellix IPS Central Manager service. In the Windows based Manager, 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 Trellix IPS Central Manager and select Stop. In the Linux based Manager, log in to the Manager shell and stop the service using the **manager stop** command.
2. Stop the Trellix IPS Central Manager Watchdog service. In the Windows based Manager, 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 Trellix IPS Central Manager Watchdog and select Stop. In the Linux based Manager, log in to the Manager shell and stop the service using the **watchdog stop** command.

### Note

Make sure the Trellix IPS Manager database service remains started.

3. In case of Windows based Manager, exit the Central Manager tray from the Windows Task Bar.
4. Close all open applications. (If any application is interacting with Trellix IPS, 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_Dir>\App\REPORTS`
6. Upgrade the Central Manager as described in [Standalone Manager on windows operating system upgrade](#) for Central Manager running on windows server and [Standalone Manager on Linux operating system upgrade](#) for Linux based Central Manager.
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.
8. Open the Central Manager in a browser.
9. Log in to the Central Manager. You can verify the version in the Dashboard page. To complete the Central Manager upgrade, you must upgrade to the latest Signature Set. See [Upgrading the Signature Set for the Central Manager](#).

:

## Upgrade the signature set for the Central Manager

Release 11.1 and later are compatible with signature set version 11.9.x or 11.10.x depending on the Manager version installed. If you are upgrading from any 10.1.x version, during installation, the signature set bundled with the installer will be imported to the Manager automatically.

### Note

For more information on 11.1.x Manager software and compatible signature set versions, refer to Trellix Intrusion Prevention System 11.1.x release notes.

#### Steps:

1. If you have not already done so, download the most recent signature set into the Central Manager. In the Central Manager, select Manager → <Admin Domain Name> → Trellix IPS Protection Status. Then, select Signature Sets tab. The Signature Sets tab is displayed. Select Download Latest Signature Set option. See the *Trellix Intrusion Prevention System Product Guide* or the *Online Help* for the steps.
2. If you created Trellix IPS custom attacks prior to upgrade, verify that those attacks are present in the Custom Attack Editor.
3. Select Manager → 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.

Signature Set upgrade is now complete for the Central Manager. For a list of currently supported protocols, see KnowledgeBase article [KB61036](#) in the [Trellix Support Portal](#).

#### What is the next step?

- If you have a Central Manager MDR, refer to section [MDR Central Manager upgrade](#).
- If you have upgraded both primary and secondary or if you have only a standalone Central Manager, upgrade the corresponding Managers.

:

### MDR Central Manager upgrade

#### Prerequisite:

Make sure both the Central Managers meet the required system requirements as mentioned in [Central Manager system requirements](#).

#### Steps:

This section provides the steps to upgrade the primary and secondary Central Managers configured for Manager Disaster Recovery (MDR).

1. Using the Suspend MDR feature, suspend the MDR pair. Click Manager and select the root admin domain. Then go to Setup → MDR → Suspend MDR.
2. Upgrade the primary Central Manager to the latest 11.1 version.
3. Upgrade the secondary Central Manager to the latest 11.1 version.
4. Using the Resume MDR feature, make the primary the active Central Manager. Make sure the latest signature set is present in both the Central Managers.

:



## How to Upgrade the Manager?

This chapter provides detailed explanation on how to upgrade the Manager to the latest 11.1 version. You must upgrade the Manager before you can upgrade the devices.

:

### Upgrade requirements for the Manager

Verify the requirements for a Manager upgrade.

:

### Upgrade path for the Manager

A direct upgrade to Central Manager or Manager 11.1 from versions earlier than what is mentioned in this section is not supported.

#### Upgrade paths for Windows based Manager software versions

Required Central Manager/Manager versions

Version	Upgrade path to 11.1
10.1.7.4, 10.1.7.7, 10.1.7.29, 10.1.7.35, 10.1.7.40, 10.1.7.44, 10.1.7.50, 10.1.7.50.2, 10.1.7.55, 10.1.7.61, 10.1.7.65, 10.1.7.66.3, 10.1.7.66.11	11.1.7.71
11.1.7.3, 11.1.7.3.5, 11.1.7.26, 11.1.7.41, 11.1.7.41.2, 11.1.7.56	11.1.7.71

#### Important

If you are using a hotfix release, contact Trellix support for the recommended upgrade path.

#### Upgrade paths for Linux based Manager software versions

### Caution

After upgrade, the Linux-based Manager reboot automatically. If it fails to reboot, check the installation logs for errors and reboot the Manager manually.

Version	Upgrade path to 11.1
10.1.7.4, 10.1.7.7, 10.1.7.25 (Cloud), 10.1.7.29, 10.1.7.35, 10.1.7.40, 10.1.7.44, 10.1.7.50, 10.1.7.50.2, 10.1.7.55, 10.1.7.61, 10.1.7.65, 10.1.7.66 (Cloud), 10.1.7.66.3, 10.1.7.66.11	11.1.7.71
11.1.7.3, 11.1.7.3.5, 11.1.7.26, 11.1.7.41, 11.1.7.41.2, 11.1.7.56	11.1.7.71

### Note

For all direct upgrades to 11.1.7.71, use the **IPSM\_111771\_setup.bin** Version **11.1.7.71** upgrade file.

### Important

If you are using a hotfix release, contact Trellix support for the recommended upgrade path.

:

## Considerations for Linux based Central Manager/Manager

Make sure to review all considerations mentioned in this section before you proceed with Linux based Manager installation or upgrade :

- In a Linux based MDR pair, both Primary and Secondary Managers should be Linux based. For example, you cannot create an MDR pair, if your Primary Manager is Windows based and Secondary Manager is Linux based or vice versa.
- The Linux based Central Manager can only manage the Linux based Managers.
- The Linux based Central Manager must be of the same or a higher version than the corresponding Linux based Managers.

:

## 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.

### Note




These suggestions do not take into account the amount of disk space you require for alert and packet log storage. See the *Trellix Intrusion Prevention System Product Guide* for suggestions on calculating your database capacity requirements.

The following table lists the 11.1 Windows based Manager/Central Manager application requirements:

### Note

Windows Server 2012 Standard/Windows Server 2012 R2 Standard is not supported for the Manager.

	Minimum required	Recommended
Operating system	<p>Any of the following:</p> <ul style="list-style-type: none"><li>• Windows Server 2016 Standard Edition English operating system</li><li>• Windows Server 2016 Standard Edition Japanese operating system</li><li>• Windows Server 2016 Datacenter Edition English operating system</li><li>• Windows Server 2016 Datacenter Edition Japanese operating system</li><li>• Windows Server 2019 Standard Edition English operating system</li><li>• Windows Server 2019 Standard Edition Japanese operating system</li><li>• Windows Server 2019 Datacenter Edition English operating system</li><li>• Windows Server 2019 Datacenter Edition Japanese operating system</li></ul>	Windows Server 2022 Datacenter Edition operating system

	Minimum required	Recommended
	<ul style="list-style-type: none"> <li>Windows Server 2022 Standard Edition English operating system</li> <li>Windows Server 2022 Standard Edition Japanese operating system</li> <li>Windows Server 2022 Datacenter Edition English operating system</li> <li>Windows Server 2022 Datacenter Edition Japanese operating system</li> </ul> <div style="background-color: #e1f5fe; padding: 5px; margin-top: 10px;">  <b>Note:</b> Only x64 architecture is supported.         </div>	
Memory	16 GB <div style="background-color: #e1f5fe; padding: 5px; margin-top: 10px;">  <b>Note:</b> Supports up to 10 million alerts in Solr           </div>	>=32 GB <div style="background-color: #e1f5fe; padding: 5px; margin-top: 10px;">  <b>Note:</b> Supports up to 20 million alerts in Solr           </div>
CPU	Server model processor, such as Intel Xeon	Same
Disk space	300 GB	500 GB or more
Network	1 Gbps card	1 Gbps card
Virtual CPUs (Applicable only on a VMware platform)	4	4 or more


 **Note**

You need Windows Administrator permission for the server machine.

### Tip


The *Trellix Intrusion Prevention System Product Guide* provides a number of pre-installation tips and suggestions with which Trellix recommends you to 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 table lists the 11.1 Linux based Manager/Central Manager application specifications for an OVA file:

Component	Specifications
MLOS	3.9.1
Logical CPU cores	8
Memory	32 GB
Disk space	500 GB
NIC	1   <b>Note:</b> You can consider 2 for a dual NIC configuration.


### How to host the Manager on a VMware platform

VMware ESXi server requirements for Windows Operating System

Component	Supported
Virtualization software	<ul style="list-style-type: none"><li>• ESXi 7.0 Update 3</li><li>• ESXi 8.0</li></ul>  <b>Note:</b> Hyperthreading should be available.

The following are the system requirements for hosting 11.1 Linux based Manager/Central Manager application on a VMware platform:

VMware ESXi server requirements for MLOS

Component	Supported
Virtualization software	<ul style="list-style-type: none"><li>ESXi 7.0 Update 3</li><li>ESXi 8.0</li></ul> <div style="background-color: #e0f2f7; padding: 5px;"> <b>Note:</b> Hyperthreading should be available.</div>

### How to host the Manager on KVM

The following table lists the 11.1 Linux based Manager/Central Manager application specifications for a qcow2 file:

Component	Specifications
MLOS	3.9.1
Logical CPU cores	8
Memory	20 GB
Disk space	500 GB
NIC	1

The following are the system requirements for hosting 11.1 Linux based Manager/Central Manager application on KVM:

KVM server requirements for MLOS

Component	Supported
Virtualization software	KVM 2.12.0

:

### Preparation for the upgrade

After you make sure you meet the requirements, prepare for the upgrade.

#### Caution

Before you begin the upgrade, make sure that no processes related to Trellix IPS (such as automated database archival) are scheduled during the upgrade time frame. Any such concurrent activity might cause conflicts and result in upgrade failure.

Make sure to review all considerations mentioned in this section before you proceed with the upgrade.

:

### 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 upgrade process of the Manager itself may take an hour to complete.

- Operating system upgrade downtime — The latest Manager 11.1 is supported on various operating systems as mentioned in [Central Manager and Manager system requirements](#). If you want to upgrade the operating system of your Manager server, 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 upgrade) continues to inspect traffic and accumulate the latest alerts (up to 100,000 alerts) while the Manager is offline during the 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 if you encounter any problem during the upgrade. Backing up immediately following the upgrade preserves your upgraded tables and provides a baseline of the 11.1 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 Trellix IPS data](#) .

### Note

You cannot restore the database from a lower version of the Manager on a higher version of the Manager.

:

## Notes for upgrading the Manager from 10.1 or 11.1 to 11.1.7.71

If you are upgrading the Manager from version 10.1 or 11.1 to version 11.1.7.71, read the following sections carefully.

### IPS support for multiple IVX brokers

Previously, IPS allowed users to integrate with a single IVX appliance broker node for malware analysis of files. Starting with this release of 11.1, IPS allows users to configure up to 5 IVX appliance broker nodes under the cluster. The Sensor submits files to the broker nodes in round robin manner for analysis and result polling, meaning better file submission rate and high availability are achieved.

Also, users can now configure broker nodes on IPv6 addresses unlike the earlier releases which supported only IPv4 communications.

In case of failed Manager-IVX or Sensor-IVX authentication, users can now view failure reason on the Manager UI which allows them to take corrective actions to attain successful authentication.

### Note

At Device level, if you are inheriting admin domain configuration, make sure that both the Manager and the Sensor are running on software version 11.1 Update 4 or later. In case of heterogeneous scenarios where you are on a 11.1 Update 4 Manager and an older Sensor that supports only one broker node on IPv4, make sure you have added only one IPv4 broker address at Global level. If you have added an IPv6 address and the settings get inherited to the older Sensor, the file detection will not happen.

### Note

It is highly recommended that you upgrade both the Manager and Sensor to 11.1 Update 4 or later releases to utilize multiple brokers which are connected over IPv4 and IPv6 addresses.

The following Sensor CLI commands are added:

Normal Mode



Command	Description
<b>ivx lookup sha256</b>	This command performs lookup on the entered SHA256 hash and returns details such as the verdict, report id, and the query time.
<b>show ivxcloud config</b>	This command displays the IVX Cloud configuration details.
<b>show ivxcloud stats</b>	This command displays statistics specific to IVX Cloud.
<b>show ivxcloud status</b>	This command displays the connection status of the IVX Cloud.

The following Sensor CLI commands are updated:

#### Normal Mode

Command	Description
<b>show ivx config</b>	This command now displays the configuration details of all the IVX broker nodes attached to the Sensor.
<b>show ivx stats brokerid</b>	This command now displays the statistics specific to the IVX broker nodes attached to the Sensor.
<b>show ivx status brokerid</b>	This command now displays the connection status of the IVX broker nodes attached to the Sensor.

The following Sensor CLI command is updated:

#### Debug Mode

Command	Description
<code>show mgmtcfg</code>	This command now displays the IVX broker node management configuration.

### Device software deployment improvements in the Manager

In this release of 11.1, several enhancements have been made on the IPS Manager to improve and speed up the device software deployment operations. This is to cater to the bulk deployment requirements of network environments where large or very large number of Sensors are deployed. The Manager takes the following actions while handling bulk Sensor software upgrade requests:

- The Manager reserves 100 GB under required free disk space for Manager operations and considers an additional file size of 1.2 GB to be generated for each software deployment request. When the Manager receives the software deployment requests in batches, it checks the number of Sensors selected, and calculates the free disk space required to complete the deployment operation. If there is insufficient disk space, an error message is displayed in the UI stating the available disk space and space required to complete the upgrade task. This enables the Manager to maintain optimal performance, secure sufficient disk space to keep other processes running, and avoid any software upgrade failure scenario.
- Software deployments are critical operations and performed under approved/scheduled maintenance window. If the Manager receives multiple deployment requests in queue along with device software update requests, such as signature file and SSL keys deployments, it prioritizes the software deployment requests ahead of all other requests. It also performs disk usage optimization for each deployment to help you perform more deployments at a faster speed, and complete the critical task of software deployments within the approved/scheduled maintenance time.

#### Note

Very large Sensor deployments mean that the number of Sensors deployed is more than 100. Large Sensor deployments have Sensors numbering between 36 and 100+.



### Deployment of IPS Manager on Kernel-based Virtual Machine (KVM)



Starting with this release of 11.1, users can deploy IPS Manager on Kernel-based Virtual Machine (KVM) using respective qcow2 image available in the [Trellix Download Server](#).

Refer to the table *KVM server requirements for MLOS* in the *Installation Parameters* section to understand the server requirements for Manager deployments on KVM.

### Terminology updates in the UI

This release contains the following terminology updates in the Manager UI:

Navigation Path	Prior to 11.1.7.71	11.1.7.71 and later
<p>Devices → &lt;Admin Domain Name&gt; → Global → IPS Device Settings → IVX Integration</p>	<p>Enable Enable MVX Integration check-box and select Enable VX.</p> <ul style="list-style-type: none"> <li>To add a broker node, enter the details of the broker node and click Save.</li> <li>To edit a broker node, update the details and click Save.</li> </ul>	<p>Enable Enable IVX Integration check-box and select Enable IVX.</p> <ul style="list-style-type: none"> <li>Click Add IVX Cluster. To add broker nodes, click the  icon located at the at the bottom-left corner of the page. The Add Broker Node panel opens to the right of the page. Enter the broker node details and click Add. Then, click Next. In the IVX Integration parent page, click Save.</li> <li>To modify a broker node in the cluster, double-click the cluster. Double-click the broker node that you want to modify. The Add Broker Node panel opens to the right of the page. Update the IVX broker details and click Update. Then, click Next. In the IVX Integration parent page, click Save.</li> <li>To delete a broker node in the cluster, double-click the cluster. Choose the broker node that you want to delete and click . Then, click Next. In the IVX Integration parent page, click Save.</li> </ul>
<p>Devices → &lt;Admin Domain Name&gt; → Devices → Setup → IVX Integration</p>	<p>Disable Inherit Settings? check-box, enable Enable MVX Integration check-box, and select Enable VX.</p>	<p>Disable Inherit Settings? check-box, enable Enable IVX Integration check-box, and select Enable IVX.</p>

Navigation Path	Prior to 11.1.7.71	11.1.7.71 and later
	<ul style="list-style-type: none"> <li>• To add a broker node, enter the details of the broker node and click Save.</li> <li>• To edit a broker node, update the details and click Save.</li> </ul>	<ul style="list-style-type: none"> <li>• Click Add IVX Cluster. To add broker nodes, click the  icon located at the at the bottom-left corner of the page. The Add Broker Node panel opens to the right of the page. Enter the broker node details and click Add. Then, click Next. In the IVX Integration parent page, click Save.</li> <li>• To modify a broker node in the cluster, double-click the cluster. Double-click the broker node that you want to modify. The Add Broker Node panel opens to the right of the page. Update the IVX broker details and click Update. Then, click Next. In the IVX Integration parent page, click Save.</li> <li>• To delete a broker node in the cluster, double-click the cluster. Choose the broker node that you want to delete and click . Then, click Next. In the IVX Integration parent page, click Save.</li> </ul>

**Rebranding updates**

This is solely for informational purpose, there is no action required. You will notice the following changes:

- Trellix Vector Execution is renamed to Trellix Intelligent Virtual Execution - Server (Trellix VX/ IVX) and Trellix Detection as a Service is renamed to Trellix Intelligent Virtual Execution Cloud (Trellix IVX Cloud/ IVX Cloud). The associated software, hardware, features, and options bearing the old product name are renamed to the new product name.
- Trellix Investigation Analysis is renamed to Trellix Network Investigator (NI). The associated software, hardware, features, and options bearing the old product name are renamed to the new product name.

This release provides the following enhancements related to platforms, environments, or operating systems:

### Apache Tomcat server upgrade

Starting with this release of 11.1, Tomcat server used in the IPS Manager is upgraded to version 9.0.83 which provides a collection of security fixes.

### JDK upgrade

Starting with this release of 11.1, the IPS Manager uses JDK version 8u392 that includes additional security against new vulnerabilities.

:

## Notes for upgrading the Manager from 10.1 or 11.1 to 11.1.7.56

If you are upgrading the Manager from version 10.1 or 11.1 to version 11.1.7.56, read the following sections carefully.

### Support for HTTP2 based traffic inspection

Starting with this release of 11.1, the Trellix IPS supports HTTP2 inspection for the following scenarios:

- HTTP2 Prior Knowledge
- Externally decrypted HTTP2 over TLS

### Note

HTTP2 upgrade (h2c) scenario is not supported.

When you install/upgrade the Manager, by default, HTTP2 traffic inspection is not enabled. You can enable HTTP2 traffic inspection at both Global and Devices level in the Manager.

Few points to consider prior to enabling the HTTP2 traffic inspection:

- The Sensor requires a reboot when you enable or disable HTTP2 Traffic Scanning. You can check the Sensor reboot status from Device Manager or **status** CLI.
- HTTP2 Traffic Scanning can be enabled only when HTTP Response Traffic Scanning is enabled.
- HTTP2 Server Push Traffic Scanning can be enabled only when HTTP2 Traffic Scanning is enabled.
- HTTP2 traffic inspection requires a sigset with HTTP2 features.
- Only NS7500 and NS9500 Sensors support HTTP2 traffic inspection.
- HTTP2 performance numbers align with HTTP 1.1 for supported Sensor models.

### Defining and enforcing user-specific blocking strategy to make self-adaptable IPS policies

Previously, if users wanted any attack to be blocked as per their blocking strategy, they had to identify all matching attacks during IPS Policy configuration, bulk edit them, and manually set the Sensor Actions to Enable Blocking. Also, they had to identify the

attack signatures that were added or modified in a new signature set release and reconfigure their IPS policies to enable the Sensor blocking response action for the attack signatures that matched their blocking criteria.

Starting with this release of 11.1, Trellix IPS Manager offers a more simplified and automated IPS policy management mechanism for blocking attacks. It enables users to define and store one or more customizable rules for blocking attacks as per their network requirements during attack set profile configuration. When the same attack set profile is used in the IPS policy, the Manager automatically correlates the blocking criteria set by the user with the new and existing attack signatures. This enables IPS policies to automatically block attacks that match the user's blocking strategy and makes them self-adaptable to any new signature set release.

This automated IPS policy management for blocking attacks minimizes the need to manually edit the IPS policies for the blocking of attacks. Moreover, as the attack set profile mapped to the IPS policy stores the user-defined blocking criteria for attacks, it is automatically applied to any new/modified attack definitions included in any signature set update that match the set criteria. This eliminates the requirement of repeated manual intervention and provides user-customizable and automated attack blocking mechanism that helps users maintain their network security posture.

You need to perform the following steps to automate the process of blocking attacks in the Manager and Sensor:

- Create or edit an attack set profile that includes rules for blocking attacks as per your blocking strategy. On the Attacks to Block tab during attack set profile configuration, you can create one or more rules with the categories, subcategories and minimum severity level of attacks that you want to be explicitly blocked by the Sensor.
- Once the attack set profile with your blocking criteria is configured, you can use the same attack set profile during IPS policy configuration. Double-clicking any attack that falls under your blocking criteria and is set to be automatically blocked shows the Block field under Sensor Actions - Response to be Inherit (Enable Blocking). This Sensor response action is only visible for attacks that are set to be automatically blocked in the selected attack set profile.

### Important

If you wish, you can override the automatic blocking behavior of any attack by manually setting the Sensor blocking action during IPS policy configuration. Sensor response actions customized in the IPS policy always takes precedence over automatic blocking of attacks criteria set in the Attack Set Profiles page.

- Once the desired IPS policy is mapped to the attack set profile that includes the rules for attack blocking, you need to enforce the IPS policy at the interface and sub-interface level for the required Sensor(s).
- You need to then deploy these configuration changes to the required devices in the admin domain level or at a device level.

When the policy and rule updates are applied to the required Sensor(s), those automatically block all attacks that match your blocking criteria as set in the attack set profile and send an alert to the Manager.

### Note

- Automating the blocking of attacks as per user-defined blocking strategy is available in both Trellix IPS Manager and Central Manager from 11.1 Update 3 release onwards.
- The default or preconfigured attack set profiles are read-only. So, the rules for blocking can be created for custom attack set profiles only.

### Forwarding MITRE Attack Details to Syslog and SNMP servers

Starting with this release of 11.1, users can configure the Manager to forward MITRE attack details to Syslog and SNMP servers. The variables introduced to forward MITRE attack details are IV\_TACTIC, IV\_TECHNIQUE, IV\_SUBTECHNIQUE, and IV\_TTPID. Users can choose the appropriate variables while configuring the **Notification Profile**.

This release provides the following enhancements related to platforms, environments, or operating systems:

#### MariaDB upgrade

Starting with this release of 11.1, the IPS Manager uses MariaDB version 10.6.14 that includes additional security against new vulnerabilities.

#### JDK upgrade

Starting with this release of 11.1, the IPS Manager uses JDK version 8u372 that includes additional security against new vulnerabilities.

:

### Notes for upgrading the Manager from 10.1 or 11.1 to 11.1.7.41

If you are upgrading the Manager from version 10.1 or 11.1 to version 11.1.7.41, read the following sections carefully.

#### Integration with Trellix Investigation Analysis

Trellix Investigation Analysis (IA) is a security analytics solution that allows the analysis of alerts and network metadata gathered from all devices connected to it. IA provides a high-level view of the network metadata gathered over customizable dashboards supporting multiple configurations. It thus enables users to have a metadata-based view of network activities and search indexed metadata from various network protocols, which allows them to zero down on threat information critical for performing further investigation.

Starting with this release of 11.1, Trellix IPS offers integration capability with IA appliances or IA cluster, and exports netflow records and Layer 7 metadata from IPS Sensors, and alert data from IPS Manager to IA as per the configuration and filter parameters set on the IA. The alert data, L7 metadata information, and flow records exported by Trellix IPS are displayed on the Dashboard of IA's Web UI which you can review and analyze further for the detection and analysis of network threats.

You need to perform the following steps to enable integration with Trellix IA:

1. Create Client Profile using the IA Command Line Interface (CLI). During the configuration of the Client Profile, you can setup specific alert severity threshold and enable protocols for L7 metadata information which you want to be exported to IA, as per your requirement.

 **Note**

Currently, IPS Sensors support the export of L7 metadata related to HTTP, HTTPS, SMTP, and FTP protocols only to IA.

2. Create Client Group on the IA CLI which enables you to assign the required Client Profile to it. A hash token value of 32 bytes is also generated on the completion of Client Group configuration task on the IA CLI, which is used by Trellix IPS for authentication purpose.

 **Note**

You can create up to 20 Client Profiles and 10 Client Groups on an IA appliance based on your requirement.

3. Configure the required Client Groups created on the IA CLI, which includes adding details such as Client Group name, IP address of the associated IA appliance, and the authentication hash token, in the Manager.
4. Enable the association of the Client Group configured in the Manager at the domain level or device level.


 **Note**

You can configure multiple Client Groups in the Manager and enable their association per-domain or per-Sensor basis.

The following tabs are available for enabling IA integration in the Manager:

	Navigation path	Description
At Global-level	Devices → <Admin Domain Name> → Global → IPS Device Settings → IA Integration → Client Group Configuration	To configure the Client Group details in the Manager
	Devices → <Admin Domain Name> → Global → IPS Device Settings → IA Integration → Client Group Association	To enable association of any Client Group for the admin domain as well as child domains



	Navigation path	Description
		 <b>Note:</b> If you enable the IA integration at an admin domain level, all child domains and the Sensors attached to these domains inherit this settings. However, you can configure any child domain with a different Client Group as per your network requirement. Consequently, the Sensors attached to that domain will inherit the same settings, unless you opt for enabling the association of a separate Client Group with different configurations for any specific Sensor within that domain.
<b>At Device-level</b>	Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → IA Integration → Client Group Association	To enable association of any Client Group per Sensor basis within any domain

 **Note**

You must configure the Client Group details in the Manager to enable its association at the domain or device level. You can configure any Client Group by using the Client Group Configuration tab available at the Global-level, or on the Client Group Association tabs available at both domain and device levels.

Following is the list of Sensor CLI commands that have been added in support of Trellix IA integration:

**Debug Mode**

Command	Description
<b>show ia status</b>	This command displays IA feature status and communication status between Trellix IPS and Trellix

Command	Description
	IA, along with other configuration details related to IA integration.
<b>getiastats</b>	This command displays counter specifics related to IA config and metadata export.
<b>cleariastats</b>	This command clears all the IA config and metadata statistics-related counters in the Sensor.
<b>ianetflowstat</b>	This command displays internal statistics specifics related to netflow and L7 metadata from datapath side.

### Syslog and SNMP server configuration

Previously, SNMP and Syslog notification profiles were configured separately through the IPS Events, Faults, and User Activity sections. Starting with this release, a Server Configuration page has been added under Manager → <Admin Domain Name> → Setup → Notification in the Manager and Central Manager. This page acts as a standard location to configure the server profiles. These server profiles can be used to configure the Syslog and SNMP notification profiles under IPS Events/Faults/User Activity.

Previously, users were provided with an option to configure Syslog servers for IPS Events and User Activity related notifications via UDP/TCP/TCP over SSL. However, Fault notifications were configured to be communicated only through UDP channel. Starting with this release, users can choose UDP/TCP/TCP over SSL while configuring Syslog server for Fault notifications.

While configuring SNMP notifications, users now have the option to choose SHA256 Authentication Type and AES256 Encryption Type for improved security.

### Note

If you are upgrading the Manager to 11.1 Update 2 or later software versions, the Manager automatically lists any existing SNMP and Syslog servers under the respective tabs in this page. The server profile name is automatically assigned by the Manager in this format <Domain Name><event/fault/audit><profile number>. For example, you are upgrading the Manager from 11.1.7.3 to 11.1.7.41. The SNMP servers are configured for the admin domain named IPS-Denver and two child domains named IPS-Welton and IPS-Larimer. IPS-Denver has 3 existing profiles while IPS-Welton and IPS-Larimer have 2 existing profiles.

When you upgrade the Manager to 11.1.7.41 or later versions, this configuration is automatically mapped under the SNMP tab under each domain. User accessing the admin domain named IPS-Denver will be viewing the server profile names as IPS-Denverfault1, IPS-Denverfault2, and IPS-Denverfault3. User accessing the child domain IPS-Welton will be viewing 2 server profiles IPS-Weltonfault1 and IPS-Weltonfault2. Similarly, user accessing the child domain IPS-Larimer will be viewing 2 server profiles IPS-Larimerfault1 and IPS-Larimerfault2.

User accessing one domain will not be able to view the servers created in other domains.

In case user has used the same Syslog or SNMP server for IPS Events, Faults, and User Activity, three server profiles will be created under the SNMP and Syslog tabs. Users can opt to delete the duplicate entries and have only one entry assigned to all the profiles. Before deleting the duplicate entries, ensure that the associated servers are not attached to any of the Syslog or SNMP notification profiles.

### Note

Before upgrading the Manager to 11.1 Update 2 or later software versions, if user has created a Syslog server (under IPS Events page) at admin domain level and same server is used in child domains, post upgrade, the user sees profiles with the same name at both admin and child domain levels. In this case, if the user plans to remove one of the profiles from any of the domains and tries creating or updating a profile with the old name in the same domain or any other domain, an error is displayed stating the name is already in use.

### Signature set version validation during its download or manual import

The signature set's major version (i.e, its first two digits) should be equal to or higher than the IPS Manager's major version (i.e, its first two digits) for it to be compatible with the Manager. Starting with this release of 11.1, the Manager performs validation based on the signature set file's major version being equal to or higher than its major version and prevents the download or manual import of any incompatible signature set version that does not match the validation criteria. For example, any Manager running on version 11.1 Update 2 supports the download and deployment of signature set version 11.9.x.x, but not signature set version 10.8.x.x or 9.8.x.x.

### vIPS license enhancements

Starting with this release of 11.1, the Manager supports licensing of both VM5000 and VM600 Sensors. Virtual Sensors require a software license to activate the baseline throughput of 5 Gbps and 1 Gbps on VM5000 and VM600 Sensors respectively. The license is provided as a .zip or .jar file. The procured license contains the details of the Sensor's throughput. The Manager checks the compliance periodically to check the number of licenses against the Sensor's throughput.

In case of the VM5000 Sensor, 5 active licenses each of 1 Gbps is required to achieve the throughput of the Sensor. For VM600 Sensor, only 1 active 1 Gbps license is required.

 **Note**

- If you are using any VM600 Sensor and plan to upgrade the Manager to 11.1.7.41 or any later versions, ensure to assign the license to the VM600 Sensor. If the license is not assigned, you cannot deploy signature sets and policy updates to the Sensor.
- In this release of the Manager, licenses for Clusters in Public Cloud is not supported.




You can upload the license from the Licenses page in the Manager. In the Manager, go to Manager → <Admin Domain Name> → Setup → Licenses and click Virtual Sensors tab. Here, you can add a license in the Manager, assign a license to the Sensor, unassign a license from the Sensor, and remove a license from the Manager.





You can assign/unassign licenses through the following nodes in the Manager:


- VM600 Sensors - License column of Device Manager, Device Details section of <Device\_Name> panel, Summary, and Licenses.
- VM5000 Sensors - License column of Device Manager, Device Details section of <Device\_Name> panel, and Summary.

**Terminology updates in the UI**

This release contains the following terminology updates in the Manager UI:

Option	Prior to 11.1.7.41	11.1.7.41 and later
<p><b>Syslog Server Configuration</b></p>	<p>To configure a Syslog Server profile under IPS Events, navigate to Manager → &lt;Admin Domain Name&gt; → Setup → Notification → IPS Events → Syslog. Under the Syslog Notification Profiles section, click  icon or choose an existing profile and click  icon. The Add a Syslog Notification Profile page appears.</p> <ul style="list-style-type: none"> <li>• To add a server profile, click the Add button next to the Target Server drop-down menu. Add a Syslog Server Profile page appears. Enter the server details and click Save.</li> </ul>	<p>To configure a Syslog Server profile, navigate to Manager → &lt;Admin Domain Name&gt; → Setup → Notification → Server Configuration and click Syslog tab.</p> <ul style="list-style-type: none"> <li>• To add a server profile, click the  icon located at the at the bottom-left corner of the page. The Syslog Server Configuration Details panel opens to the right of the page. Enter the server details and click Save.</li> <li>• To modify an existing server profile, double-click the respective Target Server Profile Name. The Syslog Server Configuration Details panel opens to the right of the page.</li> </ul>

Option	Prior to 11.1.7.41	11.1.7.41 and later
	<ul style="list-style-type: none"> <li>To modify an existing server profile, click the Edit button next to the Target Server drop-down menu. Edit a Syslog Server Profile page appears. Update the server details and click Save.</li> <li>To delete an unused server profile, click the Delete button next to the Target Server drop-down menu.</li> </ul>	<p>Update the server details and click Save.</p> <ul style="list-style-type: none"> <li>To delete an unused server profile, select the profile and click the  icon located at the bottom-left corner of the page.</li> </ul> <p>Users can use these server profiles to configure the Syslog Notification Profiles under IPS Events/Faults/User Activity.</p>
	<p>To configure a Syslog Server profile under Faults, navigate to Manager → &lt;Admin Domain Name&gt; → Setup → Notification → Faults → Syslog. Add or update the server details and click Save.</p>	<p>The Server Configuration page acts as the standard page for configuring the Syslog and SNMP Server profiles. Hence, the terminology updates remain the same as above.</p>
	<p>To configure a Syslog Server profile under User Activity, navigate to Manager → &lt;Admin Domain Name&gt; → Setup → Notification → User Activity → Syslog. Add or update the server details and click Apply.</p>	<p>The Server Configuration page acts as the standard page for configuring the Syslog and SNMP Server profiles. Hence, the terminology updates remain the same as above.</p>
<p><b>SNMP Server Configuration</b></p>	<p>To configure SNMP Server profile, navigate to Manager → &lt;Admin Domain Name&gt; → Setup → Notification → IPS Events/Faults/ User Activity → SNMP. Under the SNMP Servers section, click the  icon or choose an existing profile and click the .</p>	<p>To configure SNMP Server profile, navigate to Manager → &lt;Admin Domain Name&gt; → Setup → Notification → Server Configuration and click SNMP tab.</p> <ul style="list-style-type: none"> <li>To add a server profile, click the  icon located at the bottom-left corner of the page. The SNMP Forwarder</li> </ul>

Option	Prior to 11.1.7.41	11.1.7.41 and later
	<p>icon. The SNMP page appears.</p> <ul style="list-style-type: none"> <li>Add or update the server details depending on the action you performed above and click Save.</li> </ul>	<p>Configuration Details panel opens to the right of the page. Enter the server details and click Save.</p> <ul style="list-style-type: none"> <li>To modify a server profile, double-click an existing profile. The SNMP Forwarder Configuration Details panel opens to the right of the page. Update the server details and click Save.</li> <li>To delete a server profile, select the unused profile and click  icon.</li> </ul> <p>Users can use these server profiles to configure the SNMP Notification Profile under IPS Events/Faults/User Activity.</p>
<p><b>Import a CSV file containing Domains</b></p>	<p>To import a CSV file, navigate to Manager → &lt;Admin Domain Name&gt; → Setup → Notification → IPS Events → SNMP, go to Other Actions menu and click Import.</p>	<p>To import a CSV file, navigate to Manager → &lt;Admin Domain Name&gt; → Setup → Notification → IPS Events → SNMP, go to Other Actions menu and click Import Custom.</p>

This release provides the following enhancements related to platforms, environments, or operating systems:

**MariaDB upgrade**

Starting with this release of 11.1, the IPS Manager uses MariaDB version 10.6.12 that includes additional security against new vulnerabilities.

**JDK upgrade**

Starting with this release of 11.1, the IPS Manager uses JDK version 8u362 that includes additional security against new vulnerabilities.

:

### Notes for upgrading the Manager from 10.1 or 11.1 to 11.1.7.26

If you are upgrading the Manager from version 10.1 or 11.1 to version 11.1.7.26, read the following sections carefully.

#### Integration with Trellix Detection as a Service

Until the previous release, Trellix IPS offered integration capability with Trellix Virtual Execution which utilizes Multi-Vector Virtual Execution (MVX) engine's technology to perform malware analysis.

Starting with this release of 11.1, Trellix IPS also offers integration capability with Trellix Detection as a Service which utilizes the MVX engine's technology to perform malware analysis on cloud.

To enable integration with Detection as a Service (DaaS):



- At Global level: Navigate to Devices → <Admin Domain Name> → Global → IPS Device Settings → MVX Integration, select Enable MVX Integration checkbox, choose Enable DaaS radio button and configure the details for the integration.
- At Device level: Navigate to Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → MVX Integration. You may select the Inherit Settings? checkbox to inherit the integration configuration from the corresponding admin domain. Or, select Enable MVX Integration checkbox, choose Enable DaaS radio button and configure the details for integration.

To select MVX malware engine in an Advanced Malware policy, go to Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → Advanced Malware. You can enable inspection by MVX for all supported file types that is, Executables, MS Office Files, PDF Files, Compressed Files, Android Application Package, Java Archive, and Flash Files.

Use the Manager to view the following information with respect to files submitted for malware analysis to MVX Engine:

Dashboard tab: Use the Top Malware Files monitor to view the blocked and unblocked detections together or filter them out separately. Additionally, you can filter data based on the confidence level of the detection as well.

Analysis tab: The following enhancements are supported in the Malware Files page:

- The overall malware confidence for a file is derived based on the results from MVX and any other malware engines configured.
- If applicable, you can view the MVX-specific details for a particular type. This is similar to how you view the details for other engines.
-  In the Malware Files page, click  next to the confidence level of MVX to view the results reported by MVX. You can also download a file that contains all the reports for the malware from MVX. This file contains detailed analysis result data and can be opened with any text editor.

Devices tab: You can view the statistics of the malware detected for a given device under Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → Traffic Statistics → Advanced Malware Analysis tab. The By Malware Engine option displays the malware detected data based on the malware engines configured for the device. This includes the malware detected data associated with the MVX engine.

A list of Sensor CLI commands have been updated to support DaaS integration.

The following Sensor CLI commands are updated:

### Normal Mode

<b>Command</b>	<b>Description (If DaaS is configured)</b>
<b>show mvx config</b>	This command can now display the DaaS configuration details.
<b>show mvx stats</b>	This command earlier displayed statistics related to VX analysis. Starting with this release, the command now has the functionality to display statistics related to DaaS analysis as well.
<b>show mvx status</b>	This command now displays the connection status of the MVX engine as enabled even if DaaS is configured.
<b>clearmalwarecache</b>	This command now allows users to clear MVX related cache entries made in the Sensor which includes DaaS entries as well.
<b>clrstat</b>	This command now clears all the statistics counters in the Sensor including the MVX counters associated with DaaS.
<b>show malwareenginestats</b>	This command now displays the malware engine statistics related to DaaS under MALWARE STATISTICS FOR MVX ENGINE section.
<b>show malwarefilestats</b>	This command now displays the malware file statistics related to DaaS.

### Debug Mode



Command	Description (If DaaS is configured)
<b>set malwareEngine</b>	This command now enables or disables MVX engine.
<b>show malwareclientstats</b>	The command now displays the malware client statistics in the scan engines including MVX engine for all supported file types.
<b>show malwareEngine status</b>	This command now displays the status of the MVX engine as enabled even if DaaS is configured.
<b>show malwareserverstats</b>	This command now displays the malware server statistics in all scan engines including MVX engine for all supported file types.

### Automatic deployment of GAM updates

Starting with this release of 11.1, Trellix IPS Manager enables you to configure and deploy Gateway antimalware engine updates to all the attached Sensors (under all domains) automatically when you upload the required GAM update file (.upd) using the Manual Import tab. You can schedule the auto-deployment of GAM updates at any time of your preference on the GAM Automatic Deployment tab under Manager → <Admin Domain Name> → Trellix IPS Protection Status. The auto-deployment of new GAM updates feature works in all the following scenarios:

- The Manager deployment is in an air-gap network environment.
- The Manager is not registered with Trellix.
- The Manager is in a proxy-disabled state (in case proxy server is used in the company network for external connection).

### Note

This feature is not applicable to NTBA or virtual NTBA devices.

### Support for SHA256 hash type in Allowed and Blocked File Hashes

Starting with this release of 11.1, Trellix IPS offers capability to add SHA256 hashes to the Allowed and Blocked lists of the File Hashes under Policy → <Admin Domain Name> → Intrusion Prevention → Exceptions → File Hashes.

### Note

- The Manager running on **11.1 Update 1** or later releases supports addition of up to 400,000 hash entries (allowed and blocked hashes combined) with a limit of 200,000 per hash type. Manager prior to **11.1 Update 1 release** supports addition of only MD5 hashes up to 100,000 entries (allowed and blocked hashes combined).
- Sensors prior to **11.1 Update 1 release** do not support SHA256 hashes. The maximum number of hashes supported (allowed and blocked hashes combined) by these Sensors is 100,000.
- Sensors running on **11.1 Update 1** or later releases support both SHA256 and MD5 hashes. NS-series Sensors support a maximum of 200,000 hashes for each hash type while IPS-VM600 Sensors support a maximum of 100,000 hashes for each hash type. If the Manager has both NS-series and virtual Sensors, entries over 100,000 in each hash type are pushed only to the NS-series Sensors. The push fails on virtual Sensors and a fault is raised which can be noticed in the Faults (Manager → Troubleshooting → Logs → Faults) tab.
- In case of heterogeneous environments, if the total MD5 hash entries exceed 100,000:
  - A limit exceed error can be seen in filetransfer.log during a bulk (full) update.
  - A fault will be raised in the Faults tab and error count will be incremented at the Sensor level during an incremental update. Refer to **show ab stats** command for more information.

### Note

A Full update is triggered when the total entries are more than 4000; else, an incremental update is triggered to all the Sensors connected to the Manager.

- In case MD5 and SHA256 hashes of the same file are added, the MD5 hash takes precedence over SHA256 hash of the file during analysis.

### Support for various instance types in the Manager

Starting with this release of 11.1, the Manager in AWS can support instance types, such as m5.xlarge, c5.xlarge, m6a.xlarge, and c6a.xlarge. The recommended instance types are m5.xlarge or c5.xlarge.

This release provides the following enhancements related to platforms, environments, or operating systems:

#### Support for Windows Server 2022 operating system

Starting with this release of 11.1, Windows Server 2022 Standard and Datacenter Editions (English and Japanese) are supported for deploying the Windows-based IPS Manager.

#### MariaDB and J-connector upgrade

Starting with this release of 11.1, the IPS Manager uses MariaDB version 10.5.18 and J-connector version 2.7.7 that includes additional security against new vulnerabilities.

#### JDK and Java upgrade

Starting with this release of 11.1, the IPS Manager uses JDK and Java version 1.8.0\_352 that includes additional security against new vulnerabilities.

### Apache Tomcat server upgrade

Starting with this release of 11.1, Tomcat server used in the IPS Manager is upgraded to version 9.0.73 which provides a collection of security fixes.

This release no longer supports the following:

Starting with this release of 11.1, references related to Trellix Cloud and Cloud Analysis and Deconstruction Services (CADS) have been removed from the documentation.

:

## Notes for upgrading the Manager from 10.1 to 11.1

If you are upgrading the Manager from version 10.1 to version 11.1, read the following sections carefully.

### MITRE based attack view in Trellix IPS Manager

Starting with this release of 11.1, the Analysis → <Admin Domain Name> → Attack Log page includes Mitre Attack Details column header which displays the adversarial Tactic, Technique, Sub-Technique and Technique/Sub-Technique ID for each alert. When looking for a specific tactic, technique, or sub-technique, you can enter any related keyword for them in the Quick Search field, or apply them as filter in the column level in Attack Log. The Description tab that appears on double-clicking an attack or alert now contains collapsible subsection named Mitre Attack Details which displays the matching Tactic, Technique, Sub-Technique, and Technique/Sub-Technique ID for the attack or alert.

#### Note

Mitre Attack Details column in Attack Log is available in both Trellix IPS Manager and Central Manager.

This 11.1 release also includes MITRE ATTACK View page in the Manager that enables you to view and analyze attacks and alerts detected by the network security appliance in the MITRE ATT&CK matrix format. It offers a unified, comprehensive view of all adversarial tactics, techniques, sub-techniques, including those that match with the attack entries in the MITRE matrix structure. It also provides you with further drill-down capabilities, such as applying filters based on the attack severity level or IP address, and delving into any specific technique/sub-technique to view only the attacks that fall under those categories. You can access this page from Analysis → <Admin Domain Name> → MITRE ATTACK View.

#### Note

Mitre attack related details are not shown for older alerts.

 Note

The MITRE ATTACK View page is not available in Trellix IPS Central Manager.

**Configure rsyslog server communication with a different port in Linux-based Manager**

Starting with this release of 11.1, you can establish communication by defining the required port using **semanage**. You can define the required port for rsyslog server connection in Linux-based Manager for UDP, TCP, and TCP over SSL protocols. To establish a rsyslog connection using a required port, execute **semanage port -a -t syslogd\_port\_t -p <protocol> <port number>**. This command creates a new policy to allow the newly defined ports for the rsyslog service/configuration.



**Scheduler Details update**







Starting with this release of 11.1, Scheduler Details page is exposed in the Manager to view overall scheduled process. You can access this page from Manager → <Admin Domain Name> → Maintenance → Scheduler Details. It includes data backups, database maintenance, file maintenance, and other actions. Based on this information, you can choose an appropriate time for the backup you are currently scheduling.

**Interface name update in Port Throughput Usage**

Starting with this release of 11.1, the Manager provides a capability to view interface name by selecting the required interface displayed at the bottom of the chart. You can access these details from Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → Performance Charts. Select Throughput tab. Now, select Port Throughput Usage Mbps from drop-down. For any selected interface, you can view the details of Port <port number> (Interface: <interface name>), Port throughput rate in Mbps and time in MMM DD HH:MM:SS YYYY.

This release contains the following terminology updates in the Manager UI:

Navigation Path	Prior to 11.1.7.3	11.1.7.3 and later
Devices → <Admin Domain Name> → Global → Common Device Settings → NTP	Select Enable NTP, configure the required NTP server(s) and click Save.	Select Enable NTP and click  to configure NTP server. After adding the details, click Save.
	To remove any configured NTP server, deselect the Enable NTP and click Save.	To remove any configured NTP server, select the checkbox beside NTP Server-<number> and click  .

Navigation Path	Prior to 11.1.7.3	11.1.7.3 and later
	<p> <b>Note:</b> The Manager allows you to configure a maximum of two NTP servers with the same IP address format (i.e., IPv4 or IPv6). If you configure both NTP servers, NTP Server-1 takes a higher priority.</p>	<p> <b>Note:</b> The Manager allows you to configure a maximum of two NTP servers with the same IP address format (i.e., IPv4 or IPv6). If you configure both NTP servers, NTP Server-1 takes a higher priority.</p>
<p>Devices → &lt;Admin Domain Name&gt; → Devices → &lt;Device Name&gt; → Setup → NTP</p>	<p>Select Enable NTP, configure the required NTP server(s) and click Save.</p>	<p>Select Enable NTP and click  to configure NTP server. After adding the details, click Save.</p>
	<p>To remove any configured NTP server, deselect the Enable NTP and click Save.</p> <p> <b>Note:</b> The Manager allows you to configure a maximum of two NTP servers with the same IP address format (i.e., IPv4 or IPv6). If you configure both NTP servers, NTP Server-1 takes a higher priority.</p>	<p>To remove any configured NTP server, select the checkbox beside NTP Server-&lt;number&gt; and click  .</p> <p> <b>Note:</b> The Manager allows you to configure a maximum of two NTP servers with the same IP address format (i.e., IPv4 or IPv6). If you configure both NTP servers, NTP Server-1 takes a higher priority.</p>
<p>Manager → &lt;Admin Domain Name&gt; → Integration</p>	<p>To enable automatic import of Vulnerability Assessment Report, go to Manager → &lt;Admin Domain Name&gt; → Integration → Vulnerability Assessment → Non-MVM Report Import.</p>	<p>To enable automatic import of Vulnerability Assessment Report, go to Manager → &lt;Admin Domain Name&gt; → Integration → Vulnerability Assessment Report Import.</p>

This release provides the following enhancements related to platforms, environments, or operating systems:

### MLOS upgrade

Starting with this release of 11.1, the IPS Manager uses MLOS version 3.9.1 that includes additional security against new vulnerabilities.

### Apache Solr upgrade

With this release the IPS Manager uses Apache Solr version 8.11.2 that includes additional security against new vulnerabilities.

### Apache Tomcat upgrade

Starting with this release of 11.1, the IPS Manager uses Tomcat version 9.0.68 that includes additional security against new vulnerabilities and bug fixes.

The following Manager shell command is added:

Command	Description
<code>semanage port -a -t syslogd_port_t -p &lt;protocol&gt; &lt;port number&gt;</code>	This command creates a new policy to allow the newly defined ports for the rsyslog service/ configuration.

This release no longer supports the following:

### Support for 9.1 and 9.2 software

Starting with this release of 11.1, support for 9.1 and 9.2 software has been deprecated. Any deployments containing these software will not be supported.

### Note

If you plan to upgrade your deployments from 9.x to 11.1, you need to first upgrade your deployments to 10.1.7.65 (for Manager) and 10.1.5.190 (for Sensor) and then upgrade to 11.1.

### Integration with McAfee Vulnerability Manager

Starting with this release of 11.1, McAfee Vulnerability Manager integration has been removed since it reached End Of Life (EOL).

### Integration with Host Intrusion Prevention

Starting with this release of 11.1, Host Intrusion Prevention integration has been removed since it reached EOL.

:

### Backing up Trellix IPS data

Before you upgrade, back up your tables and save any Trellix IPS custom attacks 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.

#### Note

Save your entire backup in a different location than the current Central Manager or Manager to prevent data loss.

After you back up the Trellix IPS data, you can consider purging the Manager tables. Details on how to purge the database tables are in the *Trellix Intrusion Prevention System Product 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. Trellix 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, Trellix 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 *Trellix Intrusion Prevention System Product Guide*.

:

### Back up Trellix IPS custom attacks

If you have Trellix IPS custom attacks, back them up prior to upgrade. Refer to the corresponding version of the *Trellix Intrusion Prevention System Product Guide* for information on how to back up custom attacks from the Central Manager and Manager.

:

### Operating system upgrade for Windows based Manager

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 Windows based 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.

#### Note

The operating system upgrade is not supported on the Linux based Manager/Central Manager.

#### Note

For information on how to upgrade the operating system, refer to Microsoft's documentation.

:

### Manager and operating system upgrade

The 11.1 Manager is supported on Windows Server 2016 as mentioned in [Central Manager and Manager system requirements](#).

If you plan to upgrade the operating system to a supported flavor of Windows Server 2016, you can consider the approaches discussed in the subsequent sections.

:

### Approach 1: Upgrade the operating system and the Manager

#### Prerequisites:

- It is assumed that your 9.x Manager server is on Windows Server 2012, English or Japanese.
- It is assumed that your 9.x Manager server meets the requirements for the corresponding English or Japanese versions of Windows Server 2016.
- Note that a typical operating system upgrade can take around an hour. So, the Manager upgrade downtime window would extend till that time.

#### Steps:

1. Back up the 9.x database. See [Backing up Trellix IPS data](#).
2. Upgrade the Manager to the 10.1 version. See [MDR Manager upgrade](#) or [Stand-alone Manager upgrade](#) as per your deployment. In case of Central Manager, see [MDR Central Manager upgrade](#) or [Stand-alone Central Manager upgrade](#).



3. Log in to the Manager and go to Manager → <Admin Domain Name> → Troubleshooting → Logs. Check the Faults tab to ensure everything is working fine.

### Note

For MDR, complete these steps for one of the Managers and then proceed to the other.

4. Upgrade the operating system to English or Japanese version of the corresponding Windows Server 2016.
5. Log in to the Manager and go to Manager → <Admin Domain Name> → Troubleshooting → Logs. Check the Faults tab to ensure everything is working fine. If everything is working fine, it means that the upgrade was successful.
6. Back up the 10.1 Manager database. This backup is the baseline of your 10.1 Manager.

:

## Approach 2: Using new hardware

### Prerequisites:

- It is assumed that you have a system installed with the required Windows Server 2016 flavor.
- It is assumed that this system meets the other requirements discussed in [Reviewing the upgrade requirements](#).
- It is assumed that the 9.x Manager version meets the requirement to upgrade to 10.1. If not, first upgrade the Manager to the required 9.x version.

### Steps:

1. Back up the 9.x database. See [Backing up Trellix IPS data](#).
2. Upgrade the Manager to the latest 10.1 version. See [MDR Manager upgrade](#) or [standalone Manager upgrade](#) according to your deployment. If Central Manager, see [MDR Central Manager upgrade](#) or [Stand-alone Central Manager upgrade](#).
3. Back up the 10.1 Manager database.
4. On the new Windows Server 2016 server, install the same version of 10.1 Manager as in step-2.
5. On the network, replace the existing 9.x Manager server with the new 10.1 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.

### Note

Trellix recommends to shut down the 9.x Manager server before assigning the same IP address to the new 10.1 Manager.

6. Restore the 10.1 database backup from the old 9.x Manager on the new 10.1 Manager. For information about how to restore a database, see the latest *Trellix Intrusion Prevention System Product Guide*.
7. Log on to the new 10.1 Manager and go to Manager → <Admin Domain Name> → Troubleshooting → Logs. Check the Faults tab to make sure everything works fine.
8. Back up the 10.1 database of the Manager server. See [Performing a database backup](#).

### Note

In case of MDR, complete this procedure fully for one Manager before you proceed to the next.

:

## Standalone Manager upgrade on Windows operating system

### Prerequisites:

- If you are using Central Manager, it must be upgraded to 11.1 before you upgrade the Manager.
- Your current Trellix IPS infrastructure meets all the requirements discussed in [Reviewing the upgrade requirements](#).
- 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 [Reviewing the Upgrade Considerations](#).
- You have backed up your current Manager data. See [Performing a database backup](#).
- 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 11.1 Manager installable file at hand. You can download it from the Trellix Download Server.
- You have your Manager database 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 Manager database. The Manager cannot upgrade the database if the database is actively communicating with another application.

### Important

If this is an upgrade of a Manager in an MDR pair, then you should switch the primary Manager to standby mode before you upgrade. Make sure you are following the steps in [MDR Manager upgrade](#).

The following are the tasks to upgrade a standalone Manager.

### Steps:

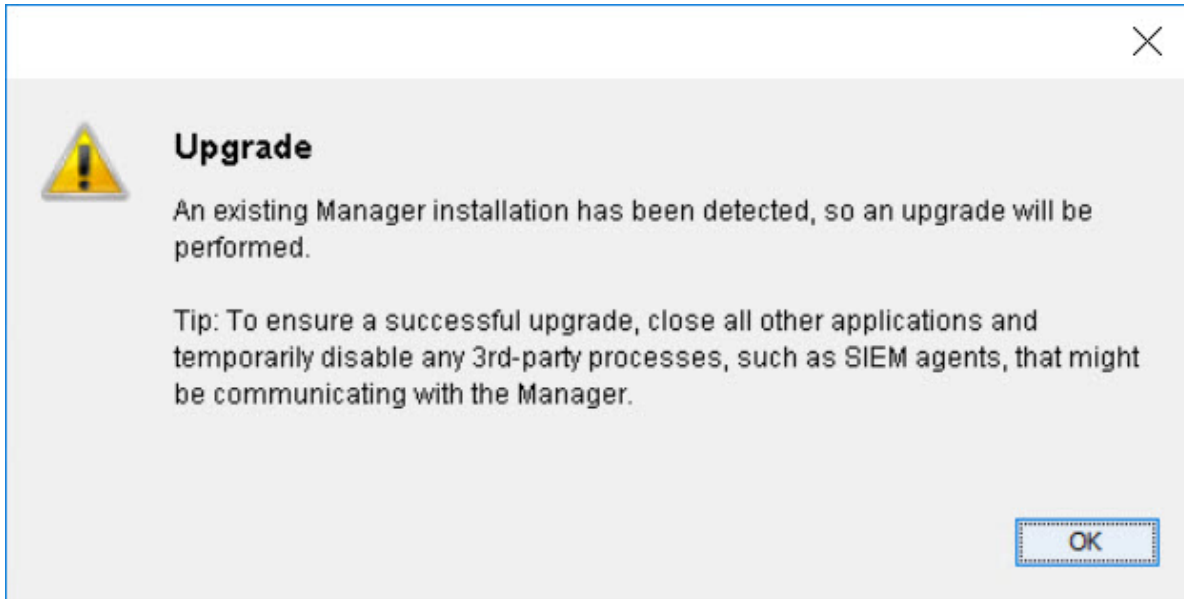
1. Stop the Manager service. Right-click on the Manager icon at the bottom-right corner of your server and stop the service. Alternatively, go to Windows Control Panel → Administrative Tools → Services. Then right-click on Trellix IPS Manager and click Stop.
2. Stop the Trellix IPS Manager Watchdog service using the same method as described to stop the Manager service.

### Note

Make sure the Trellix IPS Manager Database service remains started.

3. Exit the Manager tray from the Windows Task Bar.

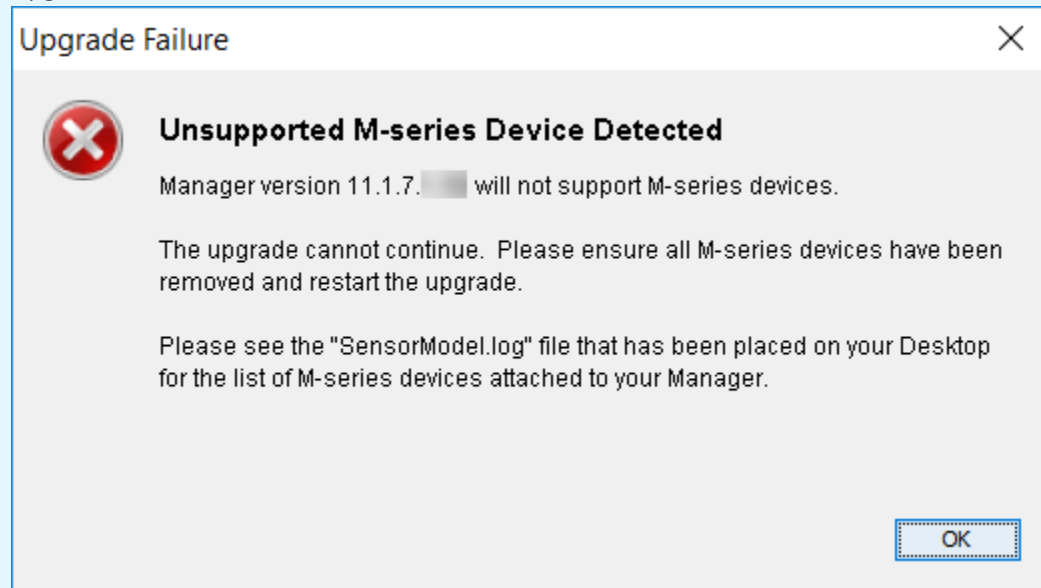
4. Move any saved report files and alert archives from the server to some other location. The reports are saved at <Manager\_Install\_Dir>\REPORTS folder. The alert archives are saved at <Manager\_Install\_Dir>\App\alertarchival folder.
5. Run the 11.1 Manager executable.
6. Close all applications communicating or running on the Windows server. Ensure that you have closed all applications and temporarily disabled any 3rd-party process, such as SIEM agents, that might be communicating with the Manager. The manager installer wizard displays the following warning message to recommend you to close all the applications.



### Caution

After providing the MariaDB password, you will not be able to proceed with the upgrade process if you have configured any M-series Sensor in the Manager. An Upgrade Failure error is displayed:

#### Upgrade Failure



To continue with the upgrade process, disconnect any M-series Sensors configured in the 10.1 Manager and restart the upgrade process.

### Important

- You can generate configuration reports for a selected M-series Sensor for future reference from Manager → <Admin Domain Name> → Reporting → Configuration Reports → IPS Sensor. For more information, see [Generate IPS Sensor reports in Trellix Intrusion Prevention System 11.1.x Product Guide](#).
- A list of all M-series Sensors are provided in SensorModel.log file on desktop. To view the complete domain path for the required M-series Sensors, go to Devices → <Admin Domain Name> → Global → Device Manager. Select the required M-series Sensor from Sensors tab and view the domain details from Owner Domain column. By default, the Owner Domain column is not enabled. To enable it, go to Device Details drop-down and select Columns → Device Details → Owner Domain.

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 the Apache Solr script on the Manager server. After the upgrade is complete, run the script only if you had been prompted to do so.
  9. Log in to the Manager. You can verify the version in the Dashboard page.
  10. Go to Manager → <Admin Domain Name> → Troubleshooting → Logs. Check the Faults tab to ensure that the Manager is up. Refer to the following sections and complete those tasks.
    1. Make sure the Manager contains the latest signature set.
    2. Upgrade the Sensor software with the latest signature set. See [Performing Signature Set and Sensor Software upgrade](#).

### Note

The default Manager root directory for App, MariaDB, and Solr will be moved from <System\_Drive>\Program Files\McAfee\Network Security Manager to <System\_Drive>\Program Files\Trellix\IPS Manager. In such scenarios, the Manager installer will prompt this directory change window. The customized root directory will remain the same.

:

## Standalone Manager upgrade on Linux operating system

Trellix recommends that you regularly monitor for maintenance releases and new versions of the Manager software. To know whether the new version of the Manager is applicable to Linux appliances, see the specific version of Trellix Intrusion Prevention System release notes. The Linux based Manager upgrade file contains Manager software upgrade file bundled with MLOS upgrade patch. On executing the Linux based Manager upgrade file, the MLOS and the Linux based Manager application are upgraded simultaneously.

### Pre-requisites:

1. Make sure you have a Linux machine installed in your network.
2. You must download the Manager upgrade file (setup.bin) from the [Download Server](#) and save it in the Linux machine, if you are upgrading from 10.1.7.4 Linux based Manager versions.

### Note

Make a note of the location where the upgrade file is saved in the Linux machine.

3. You must download the Manager upgrade file (setup.bin) from the [Download Server](#) and save it in the Linux based Manager server when using **install the setup present on local machine** upgrade in 10.1.7.7 or higher Linux based Manager versions.

### Note

Make a note of the location where the upgrade file is saved in the Manager server.

4. You must download the Manager upgrade file (setup.bin) from the [Download Server](#) and save it in the Linux machine, when using **scp setup from remote machine and install** upgrade in 10.1.7.7 or higher Linux based Manager versions.

### Note

Make a note of the location where the upgrade file is saved in the Linux machine.

### Scenario 1: If you are upgrading from Manager versions 10.1.7.4 to 10.1.7.7 and higher

1. Log on to the restricted shell of Manager Appliance using default username and password.
2. Stop the Watchdog service by executing **watchdog stop** command.
3. Stop the Manager service by executing **manager stop** command.
4. Execute the following code block to upgrade the Manager.

```
upgrade <Username> <Linux_machine_ip> <File_path_of_the_upgrade_file>
```

Following are the input parameters required for the restricted shell command:

Parameter	Description
<b>Username</b>	Login username for the Linux machine where the Manager upgrade file is saved.
<b>Linux_machine_ip</b>	IP address of Linux machine where you have saved the upgrade file.
<b>File_path_of_the_upgrade_file</b>	File path for the upgrade file in the Linux machine.

5. After executing the above command block, the Manager instance prompts a question:

```
Are you sure you want to continue connecting (yes/no)?
```

Type **yes** and press **Enter**.

6. You are prompted to provide the Linux machine password.

```
admin@w.x.y.z's password:
```

Type password for the user account and press **Enter**.

7. You are prompted to provide your Linux based Manager shell password.

```
[sudo] password for admin:
```

Type password for the Manager. By default, the password for Manager shell is **MLOSnmApp** for Manager and **MLOSnscmApp** for Central Manager.

- When you are prompted to provide the MariaDB root password, type your database root password and press **Enter**. By default, the MariaDB root password is **root123**.

### Important

After providing the MariaDB password, you will not be able to proceed with the upgrade process if you have configured any M-series Sensor in the Manager. The following error message is displayed:

```
===== Enter Database
Root password ----- Please enter Database Root password :
===== Upgrade Failure
----- Manager version 11.1.7.x will not support M-series devices. The upgrade cannot
continue. Please ensure all M-series devices have been removed and restart the upgrade. Please see
the "SensorModel.log" file that has been placed on your /opt/apps for the list of M-series devices
attached to your Manager. PRESS <ENTER> TO ACCEPT THE FOLLOWING (OK): Manager@MLOS-NSM1> dbShell
```

To continue with the upgrade process, disconnect any M-series Sensors configured in the 10.1 Manager.

### Important

- You can generate configuration reports for a selected M-series Sensor for future reference from Manager → <Admin Domain Name> → Reporting → Configuration Reports → IPS Sensor. For more information, see [Generate IPS Sensor reports in Trellix Intrusion Prevention System 11.1.x Product Guide](#).
- A list of all M-series Sensors are provided in SensorModel.log file on /opt/apps. To view the complete domain path for the required M-series Sensors, go to Devices → <Admin Domain Name> → Global → Device Manager. Select the required M-series Sensor from Sensors tab and view the domain details from Owner Domain column. By default, the Owner Domain column is not enabled. To enable it, go to Device Details drop-down and select Columns → Device Details → Owner Domain.

- After completing the upgrade procedure, check the Manager version using **show managerVersion** command to ensure successful upgrade.
- Reboot the Linux based Manager by executing **reboot** command.

### Note

The default Manager root directory for App, MariaDB, and Solr will be moved from /opt/NetworkSecurityManager to /opt/IPS Manager. In such scenarios, you will be prompted with this directory change in the console.

### Scenario 2: If you are upgrading from Manager versions 10.1.7.7 or higher

1. Log on to the restricted shell of Manager Appliance using default username and password.
2. Stop the Watchdog service by executing **watchdog stop** command.
3. Stop the Manager service by executing **manager stop** command.
4. Execute the following command to upgrade the Manager.

```
upgrade
```

5. After executing the above command, the Manager instance prompts the following options:

```
Choose one of the below options
1: scp setup from remote machine and install
2: install the setup present on local machine
Input [1] or [2] : <Select the upgrade method>
```

#### Note

If you select **1: scp setup from remote machine and install**, you must have the Linux based Manager upgrade file saved in a remote Linux machine.

#### Note

If you select **2: install the setup present on local machine**, you must have the Linux based Manager upgrade file saved in the Linux based Manager itself.

6. If you select 1, continue with the following steps, else skip to step 7.
  - a. You are prompted to provide your SCP server IP address:

```
Enter the IP of the remote machine: <remote_machine_ip>
```

Type the SCP server IP address and press **Enter**.

- b. You are prompted to provide your username for the SCP server.

```
Enter the user of the remote machine: <remote_machine_user>
```

Type your username for the SCP server and press **Enter**.

- c. You are prompted to provide the filepath of Manager upgrade file in the SCP server.

```
Enter the setup file's path as on remote machine: <Filepath of the upgrade file in the remote machine>
```

Type filepath for the upgrade file in SCP server and press **Enter**.

- d. When you are prompted to provide the MariaDB root password, type your database root password and press **Enter**.  
By default, the MariaDB root password is **root123**.



**i** Important

After providing the MariaDB password, you will not be able to proceed with the upgrade process if you have configured any M-series Sensor in the Manager. The following error message is displayed:

```
===== Enter Database
Root password ----- Please enter Database Root password :
===== Upgrade Failure
----- Manager version 11.1.7.x will not support M-series devices. The upgrade cannot
continue. Please ensure all M-series devices have been removed and restart the upgrade. Please
see the "SensorModel.log" file that has been placed on your /opt/apps for the list of M-series
devices attached to your Manager. PRESS <ENTER> TO ACCEPT THE FOLLOWING (OK): Manager@MLOS-NSM1>
dbShell
```

To continue with the upgrade process, disconnect any M-series Sensors configured in the 10.1 Manager.

**i** Important

- You can generate configuration reports for a selected M-series Sensor for future reference from Manager → <Admin Domain Name> → Reporting → Configuration Reports → IPS Sensor. For more information, see [Generate IPS Sensor reports in Trellix Intrusion Prevention System 11.1.x Product Guide](#).
- A list of all M-series Sensors are provided in SensorModel.log file on /opt/apps. To view the complete domain path for the required M-series Sensors, go to Devices → <Admin Domain Name> → Global → Device Manager. Select the required M-series Sensor from Sensors tab and view the domain details from Owner Domain column. By default, the Owner Domain column is not enabled. To enable it, go to Device Details drop-down and select Columns → Device Details → Owner Domain.

e. After completing the upgrade procedure, check the Manager version using **show managerVersion** command to ensure successful upgrade.

f. Reboot the Linux based Manager by executing **reboot** command.

7. If you select 2, do the following.

a. You are prompted to provide filepath of the upgrade file in the Linux based Manager server:

```
Enter the path to the setup.bin file: <upgrade_file_filepath>
```

Type the filepath of the upgrade file in the Linux based Manager server and press **Enter**.

b. When you are prompted to provide the MariaDB root password, type your database root password and press **Enter**. By default, the MariaDB root password is **root123**.

 **Caution**

After providing the MariaDB password, you will not be able to proceed with the upgrade process if you have configured any M-series Sensor in the Manager. The following error message is displayed:

```
===== Enter Database
Root password ----- Please enter Database Root password :
===== Upgrade Failure
----- Manager version 11.1.7.x will not support M-series devices. The upgrade cannot
continue. Please ensure all M-series devices have been removed and restart the upgrade. Please
see the "SensorModel.log" file that has been placed on your /opt/apps for the list of M-series
devices attached to your Manager. PRESS <ENTER> TO ACCEPT THE FOLLOWING (OK): Manager@MLOS-NSM1>
dbShell
```

To continue with the upgrade process, disconnect any M-series Sensors configured in the 10.1 Manager.

 **Important**

- You can generate configuration reports for a selected M-series Sensor for future reference from Manager → <Admin Domain Name> → Reporting → Configuration Reports → IPS Sensor. For more information, see [Generate IPS Sensor reports in Trellix Intrusion Prevention System 11.1.x Product Guide](#).
- A list of all M-series Sensors are provided in SensorModel.log file on /opt/apps. To view the complete domain path for the required M-series Sensors, go to Devices → <Admin Domain Name> → Global → Device Manager. Select the required M-series Sensor from Sensors tab and view the domain details from Owner Domain column. By default, the Owner Domain column is not enabled. To enable it, go to Device Details drop-down and select Columns → Device Details → Owner Domain.

- c. After completing the upgrade procedure, check the Manager version using **show managerVersion** command to ensure successful upgrade.
- d. Reboot the Linux based Manager by executing **reboot** command.

 **Note**

The default Manager root directory for App, MariaDB, and Solr will be moved from /opt/NetworkSecurityManager to /opt/IPS Manager. In such scenarios, you will be prompted with this directory change in the console.

:

## Root partition extension in Linux-based Manager

Perform the following steps to extend the root partition in the Linux-based Manager:

**Prerequisite:**

Take an ALL TABLES database backup of the Linux-based Manager and store it in a remote machine.

### Steps:

1. Log in to the Manager shell.
2. Shutdown the Manager virtual machine by executing **shutdown** command.
3. Log in to the ESXi server where the Linux-based Manager virtual machine is hosted.
4. Select the Linux-based Manager virtual machine and edit the machine setting to extend the disk space.

#### Note

Make a note of the memory size extended in gigabytes.

5. Power on the Linux-based Manager virtual machine.
6. Log in to the Manager shell.
7. Execute **fdisk -l**.

#### Note

Make a note of the output displayed on executing the above command.

8. Execute **fdisk /dev/sda**.  
The fdisk utility opens.
9. Type **p** and press **Enter**. Make a note of the end block of sda. For example: In the below output, the end block is 419239935.

```
Device Boot Start End Blocks Id System /dev/sda1 2048 780287 389120 83 Linux /dev/sda2 782336 419239935
209228800 83 Linux
```

10. Create a new partition by executing **n**.
11. The console provides options for partition type. Type **P** to select **Primary** and press **Enter**.
12. Select the partition number and press **Enter**.

#### Note

Trellix recommends you to select the default partition number displayed.

13. Select the first sector for the extended partition and press **Enter**.

#### Note

Trellix recommends you to select the first block after the end of the available sda blocks as the first sector for the extended partition. That is, if the end location of the available sda is **419239935**, then you must specify the first sector as **419239936** (i.e. **419239935+1**).

14. Select the last sector of the extended partition and press **Enter**.

 **Note**

Trellix recommends you to select the default location displayed.

15. Save the changes to the fdisk utility by executing **w**.
16. Reboot the Linux-based Manager by executing **reboot** command.
17. Log in to the Manager shell.
18. Execute **fdisk -l**.

 **Note**

Make a note of the output displayed on executing the above command.

19. Compare the output of fdisk command in step 7 and step 18. Make a note of the new sda created.
20. Execute the below command block to extend the root partition:

```
vgextend fs /dev/<new_sda>
```

Parameter	Description
<b>new_sda</b>	Specify the name of the newly created sda.

21. Execute the below command block:

```
lvextend -L+<memory_extended>G /dev/mapper/fs-root
```

Parameter	Description
<b>memory_extended</b>	Mention the memory size extended in gigabytes as specified in step 4. For example, if you have increased the disk space of the Linux-based Manager virtual machine by 50 GB, the <b>memory_extended</b> value should be entered as 50.

22. Execute **df -h** and make a note of **/dev/mapper/fs-root** filesystem size.
23. Execute the below command block to resize the **/dev/mapper/fs-root** filesystem size.

```
resize2fs /dev/mapper/fs-root
```

24. Execute **df -h** and verify that the **/dev/mapper/fs-root** filesystem size is extended.

:

### MDR Manager upgrade

#### Prerequisite:

Make sure both the Managers meet the required system requirements as mentioned in [Central Manager system requirements](#).

This section provides the steps to upgrade the primary and secondary Managers configured for Manager Disaster Recovery (MDR).

#### Note

If you are upgrading from the Manager version 9.2.7.31 or lower, or 9.2.9.8 or lower to the Manager version 9.2.9.12 or later, Trellix recommends you to suspend the MDR pair, upgrade the individual Managers and then resume the MDR pair.

#### Steps:

1. Using the Suspend MDR feature, suspend the MDR pair. Click Manager and select the root admin domain. Then go to Setup → MDR → Suspend MDR.
2. Upgrade the primary Manager to 11.1.
3. Upgrade the secondary Manager to 11.1.
4. Using the Resume MDR feature, make the primary the active Manager. Make sure the latest 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.

:

## How to perform signature set and Sensor software upgrade

This section contains information on how to upgrade the Sensors to the latest 11.1 version.

#### Important

Before you proceed with the Sensor software upgrade, you must upgrade the Manager to 11.1.

:

### Difference between an update and an upgrade

A software update is a minor release of device software. A device refers to a Sensor. 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.

### Note

Any change to device software, whether an update or upgrade, requires you to do a full reboot of the device.

:

### Signature set upgrade

Release 11.1 and later are compatible with signature set version 11.9.x or 11.10.x depending on the Manager version installed. If you are upgrading from any 10.1.x version, during installation, the signature set bundled with the installer will be imported to the Manager automatically.

### Note

For more information on 11.1.x Manager software and compatible signature set versions, refer to Trellix Intrusion Prevention System 11.1.x release notes.

### Increase in memory size for handling signature sets

With a growing number of threats, the frequency of signature set updates and the number of attacks in each update constantly increase. As a means to accommodate a larger signature set size in the future, the memory size allocated to signature sets on the Sensor has been increased.

:

### Sensor software upgrade requirements

This section details the requirements to upgrade the Sensor software to 11.1. In this section, the term *Sensor* refers to NS-series and Virtual IPS Sensors unless otherwise specified.

#### Prerequisites for NS-series Sensor software upgrade

#### Upgrade paths for NS-series Sensor software versions

Sensor models	Version	Upgrade path to 11.1
NS9500 (Standalone)	10.1.5.3, 10.1.5.5, 10.1.5.41, 10.1.5.64, 10.1.5.75, 10.1.5.92,	11.1.5.72

Sensor models	Version	Upgrade path to 11.1
	10.1.5.107, 10.1.5.116, 10.1.5.153, 10.1.5.170, 10.1.5.190, 10.1.5.204	
	11.1.5.2, 11.1.5.22, 11.1.5.44, 11.1.5.57	11.1.5.72
NS9500 (Stack)	10.1.5.3, 10.1.5.5, 10.1.5.41, 10.1.5.64, 10.1.5.75, 10.1.5.92, 10.1.5.107, 10.1.5.116, 10.1.5.153, 10.1.5.170, 10.1.5.190, 10.1.5.204	11.1.5.72
	11.1.5.2, 11.1.5.22, 11.1.5.44, 11.1.5.56	11.1.5.72
NS-series (NS9300, NS9200, NS9100, NS7300, NS7200, NS7100, NS5200, NS5100, NS3200, NS3100)	10.1.5.3, 10.1.5.5, 10.1.5.41, 10.1.5.64, 10.1.5.75, 10.1.5.92, 10.1.5.106, 10.1.5.116, 10.1.5.153, 10.1.5.170, 10.1.5.190, 10.1.5.202	11.1.5.72
	11.1.5.2, 11.1.5.22, 11.1.5.44, 11.1.5.56	11.1.5.72
NS7500	10.1.5.64, 10.1.5.75, 10.1.5.92, 10.1.5.106, 10.1.5.116, 10.1.5.153, 10.1.5.170, 10.1.5.190, 10.1.5.202	11.1.5.72
	11.1.5.2, 11.1.5.22, 11.1.5.44, 11.1.5.56	11.1.5.72
NS7x50	10.1.5.3, 10.1.5.5, 10.1.5.41, 10.1.5.64, 10.1.5.75, 10.1.5.92, 10.1.5.107, 10.1.5.116, 10.1.5.153, 10.1.5.170, 10.1.5.190, 10.1.5.204	11.1.5.72
	11.1.5.2, 11.1.5.22, 11.1.5.44, 11.1.5.57	11.1.5.72

Sensor models	Version	Upgrade path to 11.1
NS3500	10.1.5.3, 10.1.5.5, 10.1.5.41, 10.1.5.64, 10.1.5.75, 10.1.5.92, 10.1.5.106, 10.1.5.116, 10.1.5.153, 10.1.5.170, 10.1.5.190, 10.1.5.202	11.1.5.72
	11.1.5.2, 11.1.5.22, 11.1.5.44, 11.1.5.56	11.1.5.72

### Important

If you are using a hotfix release, contact Trellix Support for the recommended upgrade path.

### Important

When you perform a Sensor upgrade and reboot the Sensor, you need to verify the status of Sensor through CLI and confirm if it displays SIGFILE or NO\_SIGFILE. If the Sensor displays NO\_SIGFILE, it is in an abnormal state. You can recover the Sensor immediately by manually deploying sigfile to the Sensor using Manager.

## Prerequisites for Virtual IPS Sensor software upgrade

### Upgrade paths for Virtual IPS Sensor software versions

Sensor models	Version	Upgrade path to 11.1
IPS-VM600	10.1.7.1, 10.1.7.42, 10.1.7.51, 10.1.7.65, 10.1.7.86, 10.1.7.96, 10.1.7.123, 10.1.7.135, 10.1.7.155, 10.1.7.156 (Cloud)	11.1.7.72
	11.1.7.1, 11.1.7.22, 11.1.7.44, 11.1.7.56	11.1.7.72
IPS-VM5000	11.1.7.44, 11.1.7.56	11.1.7.72



### Important

Starting with the 11.1 Update 2 release, the minimum memory requirement for IPS-VM600 deployment on ESXi and KVM is 8 GB. Contact Trellix support for more information and assistance.

:

### Review the upgrade considerations for Sensors

Review this section carefully before you commence the upgrade process.

:

### Notes for upgrading the Sensor from 10.1 or 11.1 to 11.1.5.72

If you are upgrading the Sensor from version 10.1 or 11.1 to version 11.1.5.72, read the following sections carefully.

#### IPS support for multiple IVX brokers

Previously, IPS allowed users to integrate with a single IVX appliance broker node for malware analysis of files. Starting with this release of 11.1, IPS allows users to configure up to 5 IVX appliance broker nodes under the cluster. The Sensor submits files to the broker nodes in round robin manner for analysis and result polling, meaning better file submission rate and high availability are achieved.

Also, users can now configure broker nodes on IPv6 addresses unlike the earlier releases which supported only IPv4 communications.

In case of failed Manager-IVX or Sensor-IVX authentication, users can now view failure reason on the Manager UI which allows them to take corrective actions to attain successful authentication.

### Note

At Device level, if you are inheriting admin domain configuration, make sure that both the Manager and the Sensor are running on software version 11.1 Update 4 or later. In case of heterogeneous scenarios where you are on a 11.1 Update 4 Manager and an older Sensor that supports only one broker node on IPv4, make sure you have added only one IPv4 broker address at Global level. If you have added an IPv6 address and the settings get inherited to the older Sensor, the file detection will not happen.

### Note

It is highly recommended that you upgrade both the Manager and Sensor to 11.1 Update 4 or later releases to utilize multiple brokers which are connected over IPv4 and IPv6 addresses.

The following Sensor CLI commands are added:

## Normal Mode

Command	Description
<b>ivx lookup sha256</b>	This command performs lookup on the entered SHA256 hash and returns details such as the verdict, report id, and the query time.
<b>show ivxcloud config</b>	This command displays the IVX Cloud configuration details.
<b>show ivxcloud stats</b>	This command displays statistics specific to IVX Cloud.
<b>show ivxcloud status</b>	This command displays the connection status of the IVX Cloud.

The following Sensor CLI commands are updated:

## Normal Mode

Command	Description
<b>show ivx config</b>	This command now displays the configuration details of all the IVX broker nodes attached to the Sensor.
<b>show ivx stats brokerid</b>	This command now displays the statistics specific to the IVX broker nodes attached to the Sensor.
<b>show ivx status brokerid</b>	This command now displays the connection status of the IVX broker nodes attached to the Sensor.

The following Sensor CLI command is updated:

## Debug Mode

Command	Description
<code>show mgmtcfg</code>	This command now displays the IVX broker node management configuration.

### Device software deployment improvements in the Manager

In this release of 11.1, several enhancements have been made on the IPS Manager to improve and speed up the device software deployment operations. This is to cater to the bulk deployment requirements of network environments where large or very large number of Sensors are deployed. The Manager takes the following actions while handling bulk Sensor software upgrade requests:

- The Manager reserves 100 GB under required free disk space for Manager operations and considers an additional file size of 1.2 GB to be generated for each software deployment request. When the Manager receives the software deployment requests in batches, it checks the number of Sensors selected, and calculates the free disk space required to complete the deployment operation. If there is insufficient disk space, an error message is displayed in the UI stating the available disk space and space required to complete the upgrade task. This enables the Manager to maintain optimal performance, secure sufficient disk space to keep other processes running, and avoid any software upgrade failure scenario.
- Software deployments are critical operations and performed under approved/scheduled maintenance window. If the Manager receives multiple deployment requests in queue along with device software update requests, such as signature file and SSL keys deployments, it prioritizes the software deployment requests ahead of all other requests. It also performs disk usage optimization for each deployment to help you perform more deployments at a faster speed, and complete the critical task of software deployments within the approved/scheduled maintenance time.

#### Note

Very large Sensor deployments mean that the number of Sensors deployed is more than 100. Large Sensor deployments have Sensors numbering between 36 and 100+.

### Support for external file reputation through Trellix Threat Intelligence Exchange (TIE)

Starting with this release of 11.1, IPS allows users to integrate an external file reputation provider to the existing list of TIE providers. This will allow the sensor to receive a reputation score for the file from the External Provider.

### Cache implementation for Trellix Threat Intelligence Exchange (TIE) / Global Threat Intelligence (GTI) File Reputation

Starting with this release of 11.1, caching support is extended to Trellix TIE/GTI File Reputation service. Following Sensor CLI commands are updated for TIE/GTI cache implementation:

## Normal Mode

Command	Description
<code>clearmalwarecache</code>	This command now allows users to clear cache entries related to TIE/GTI engine made in the Sensor.
<code>malwarecache</code>	This command now enables or disables malware cache for TIE/GTI engine

## Debug Mode

Command	Description
<code>show malwareserverstats</code>	This command now includes an entry called <b>Artemis Cache hit Cnt</b> to display the number of times TIE/GTI cache is being read.

## Rebranding updates

This is solely for informational purpose, there is no action required. You will notice the following changes:

- Trellix Vector Execution is renamed to Trellix Intelligent Virtual Execution - Server (Trellix VX/ IVX) and Trellix Detection as a Service is renamed to Trellix Intelligent Virtual Execution Cloud (Trellix IVX Cloud/ IVX Cloud). The associated software, hardware, features, and options bearing the old product name are renamed to the new product name.
- Trellix Investigation Analysis is renamed to Trellix Network Investigator (NI). The associated software, hardware, features, and options bearing the old product name are renamed to the new product name.

## IPS CLI enhancements

The following Sensor CLI commands are updated:

## Normal Mode

Command	Description
<code>clearmalwarecache</code>	This command has been updated with respect to the rebranding changes made on MVX. If users plan to

Command	Description
	delete cache entries of IVX, they need to issue the command <b>clearmalwarecache ivx</b> .
<b>malwarecache</b>	This command has been updated with respect to the rebranding changes made on MVX. If users plan to enable or disable malware cache of IVX engine, they need to use the syntax <b>malwarecache &lt;enable   disable&gt; ivx</b> .

The following Sensor CLI commands are updated:

#### Debug Mode

Command	Description
<b>set malwareEngine</b>	This command has been updated with respect to the rebranding changes made on MVX. If users plan to enable/disable the IVX malware engine for Advanced Malware inspection, they need to issue the syntax <b>set malwareEngine ivx &lt;enable   disable</b> .
<b>show ni status</b>	The syntax and output of this command have been updated with respect to rebranding changes made on Trellix NI.
<b>getnistats</b>	The syntax and output of this command have been updated with respect to rebranding changes made on Trellix NI.
<b>clearnistats</b>	The syntax and output of this command have been updated with respect to rebranding changes made on Trellix NI.

Command	Description
<b>ninetflowstat</b>	The syntax and output of this command have been updated with respect to rebranding changes made on Trellix NI.

 **Note**

Apart from the above listed commands, a few more commands have been updated where the output displays the rebranding changes. As these changes do not have impact over the commands you input, they have not been listed here.

:

## Note about upgrading the Sensor from 10.1 or 11.1 to 11.1.5.56 or 11.1.5.57

If you are upgrading the Sensor from version 10.1 or 11.1 to version 11.1.5.56 or 11.1.5.57, read the following sections carefully.

### Support for HTTP2 based traffic inspection

The following Sensor CLI commands are included:

Normal Mode

Command	Description
<b>show h2 config</b>	Displays details related to HTTP2 status, flow allocation, and decoded packet status.
<b>show h2 connections</b>	Displays statistics details related to HTTP2 context connections.
<b>show h2 frames</b>	Displays multiple frames counter details and settings-frames statistics.
<b>show h2 header-decoder</b>	Displays the HTTP2 header block decode status.

Command	Description
<b>show h2 resource</b>	Displays statistics details related to available and total allocations of HTTP2 resources.
<b>show h2 streams</b>	Displays statistics details related to HTTP2 streams.

The following Sensor CLI command is updated:


Debug Mode

Command	Description
<b>show feature status</b>	Displays the enable/disable status for a certain features.

### Sensor CLI commands

Along with commands related to HTTP2 documented above, the following Sensor CLI command is updated:

Debug Mode

Command	Description
<b>show acl stats</b>	<p>Displays the count of packets matching the Stateless ACL rule which skipped the proxy engine.</p> <div style="background-color: #e0f2f7; padding: 10px; border: 1px solid #ccc;"> <p> <b>Note:</b> This counter appears in the output only when SSL Decryption on Inbound/Outbound traffic is enabled.</p> </div>

:

### Note about upgrading the Sensor from 10.1 or 11.1 to 11.1.5.44

If you are upgrading the Sensor from version 10.1 or 11.1 to version 11.1.5.44, read the following sections carefully.

#### Integration with Trellix Investigation Analysis

Trellix Investigation Analysis (IA) is a security analytics solution that allows the analysis of alerts and network metadata gathered from all devices connected to it. IA provides a high-level view of the network metadata gathered over customizable dashboards supporting multiple configurations. It thus enables users to have a metadata-based view of network activities and search indexed metadata from various network protocols, which allows them to zero down on threat information critical for performing further investigation.

Starting with this release of 11.1, Trellix IPS offers integration capability with IA appliances or IA cluster, and exports netflow records and Layer 7 metadata from IPS Sensors, and alert data from IPS Manager to IA as per the configuration and filter parameters set on the IA. The alert data, L7 metadata information, and flow records exported by Trellix IPS are displayed on the Dashboard of IA's Web UI which you can review and analyze further for the detection and analysis of network threats.

You need to perform the following steps to enable integration with Trellix IA:

1. Create Client Profile using the IA Command Line Interface (CLI). During the configuration of the Client Profile, you can setup specific alert severity threshold and enable protocols for L7 metadata information which you want to be exported to IA, as per your requirement.

#### Note

Currently, IPS Sensors support the export of L7 metadata related to HTTP, HTTPS, SMTP, and FTP protocols only to IA.

2. Create Client Group on the IA CLI which enables you to assign the required Client Profile to it. A hash token value of 32 bytes is also generated on the completion of Client Group configuration task on the IA CLI, which is used by Trellix IPS for authentication purpose.

#### Note

You can create up to 20 Client Profiles and 10 Client Groups on an IA appliance based on your requirement.


3. Configure the required Client Groups created on the IA CLI, which includes adding details such as Client Group name, IP address of the associated IA appliance, and the authentication hash token, in the Manager.
4. Enable the association of the Client Group configured in the Manager at the domain level or device level.




 **Note**

You can configure multiple Client Groups in the Manager and enable their association per-domain or per-Sensor basis.

The following tabs are available for enabling IA integration in the Manager:

	Navigation path	Description
At Global-level	Devices → <Admin Domain Name> → Global → IPS Device Settings → IA Integration → Client Group Configuration	To configure the Client Group details in the Manager
	Devices → <Admin Domain Name> → Global → IPS Device Settings → IA Integration → Client Group Association	To enable association of any Client Group for the admin domain as well as child domains   <b>Note:</b> If you enable the IA integration at an admin domain level, all child domains and the Sensors attached to these domains inherit this settings. However, you can configure any child domain with a different Client Group as per your network requirement. Consequently, the Sensors attached to that domain will inherit the same settings, unless you opt for enabling the association of a separate Client Group with different configurations for any specific Sensor within that domain.
At Device-level	Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → IA Integration → Client Group Association	To enable association of any Client Group per Sensor basis within any domain

 **Note**

You must configure the Client Group details in the Manager to enable its association at the domain or device level. You can configure any Client Group by using the Client Group Configuration tab available at the Global-level, or on the Client Group Association tabs available at both domain and device levels.

Following is the list of Sensor CLI commands that have been added in support of Trellix IA integration:

**Debug Mode**

Command	Description
<b>show ia status</b>	This command displays IA feature status and communication status between Trellix IPS and Trellix IA, along with other configuration details related to IA integration.
<b>getiastats</b>	This command displays counter specifics related to IA config and metadata export.
<b>cleariastats</b>	This command clears all the IA config and metadata statistics-related counters in the Sensor.
<b>ianetflowstat</b>	This command displays internal statistics specifics related to netflow and L7 metadata from datapath side.

**Sensor CLI commands**

Along with commands related to Trellix IA integration documented above, the following Sensor CLI command is updated:

**Debug Mode**

Command	Description
<b>rspstat</b>	Displays the datapath attack response related statistics. With this release, it also displays the number of attacks superseded by alert-correlation.

:

### Note about upgrading the Sensor from 10.1 or 11.1 to 11.1.5.22

If you are upgrading the Sensor from version 10.1 or 11.1 to version 11.1.5.22, read the following sections carefully.

#### Integration with Trellix Detection as a Service

Until the previous release, Trellix IPS offered integration capability with Trellix Virtual Execution which utilizes Multi-Vector Virtual Execution (MVX) engine's technology to perform malware analysis.

Starting with this release of 11.1, Trellix IPS also offers integration capability with Trellix Detection as a Service which utilizes the MVX engine's technology to perform malware analysis on cloud.

To enable integration with Detection as a Service (DaaS):


- At Global level: Navigate to Devices → <Admin Domain Name> → Global → IPS Device Settings → MVX Integration, select Enable MVX Integration checkbox, choose Enable DaaS radio button and configure the details for the integration.
- At Device level: Navigate to Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → MVX Integration. You may select the Inherit Settings? checkbox to inherit the integration configuration from the corresponding admin domain. Or, select Enable MVX Integration checkbox, choose Enable DaaS radio button and configure the details for integration.

To select MVX malware engine in an Advanced Malware policy, go to Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → Advanced Malware. You can enable inspection by MVX for all supported file types that is, Executables, MS Office Files, PDF Files, Compressed Files, Android Application Package, Java Archive, and Flash Files.

Use the Manager to view the following information with respect to files submitted for malware analysis to MVX Engine:

Dashboard tab: Use the Top Malware Files monitor to view the blocked and unblocked detections together or filter them out separately. Additionally, you can filter data based on the confidence level of the detection as well.

Analysis tab: The following enhancements are supported in the Malware Files page:

- The overall malware confidence for a file is derived based on the results from MVX and any other malware engines configured.
- If applicable, you can view the MVX-specific details for a particular type. This is similar to how you view the details for other engines.
- In the Malware Files page, click  next to the confidence level of MVX to view the results reported by MVX. You can also download a file that contains all the reports for the malware from MVX. This file contains detailed analysis result data and can be opened with any text editor.

Devices tab: You can view the statistics of the malware detected for a given device under Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → Traffic Statistics → Advanced Malware Analysis tab. The By Malware Engine

option displays the malware detected data based on the malware engines configured for the device. This includes the malware detected data associated with the MVX engine.

A list of Sensor CLI commands have been updated to support DaaS integration.

The following Sensor CLI commands are updated:

### Normal Mode

Command	Description (If DaaS is configured)
<b>show mvx config</b>	This command can now display the DaaS configuration details.
<b>show mvx stats</b>	This command earlier displayed statistics related to VX analysis. Starting with this release, the command now has the functionality to display statistics related to DaaS analysis as well.
<b>show mvx status</b>	This command now displays the connection status of the MVX engine as enabled even if DaaS is configured.
<b>clearmalwarecache</b>	This command now allows users to clear MVX related cache entries made in the Sensor which includes DaaS entries as well.
<b>clrstat</b>	This command now clears all the statistics counters in the Sensor including the MVX counters associated with DaaS.
<b>show malwareenginestats</b>	This command now displays the malware engine statistics related to DaaS under MALWARE STATISTICS FOR MVX ENGINE section.
<b>show malwarefilestats</b>	This command now displays the malware file statistics related to DaaS.

### Debug Mode

Command	Description (If DaaS is configured)
<b>set malwareEngine</b>	This command now enables or disables MVX engine.
<b>show malwareclientstats</b>	The command now displays the malware client statistics in the scan engines including MVX engine for all supported file types.
<b>show malwareEngine status</b>	This command now displays the status of the MVX engine as enabled even if DaaS is configured.
<b>show malwareserverstats</b>	This command now displays the malware server statistics in all scan engines including MVX engine for all supported file types.

### Support for SHA256 hash type in Allowed and Blocked File Hashes

Starting with this release of 11.1, Trellix IPS offers capability to add SHA256 hashes to the Allowed and Blocked lists of the File Hashes under Policy → <Admin Domain Name> → Intrusion Prevention → Exceptions → File Hashes.

### Note

- The Manager running on **11.1 Update 1** or later releases supports addition of up to 400,000 hash entries (allowed and blocked hashes combined) with a limit of 200,000 per hash type. Manager prior to **11.1 Update 1 release** supports addition of only MD5 hashes up to 100,000 entries (allowed and blocked hashes combined).
- Sensors prior to **11.1 Update 1 release** do not support SHA256 hashes. The maximum number of hashes supported (allowed and blocked hashes combined) by these Sensors is 100,000.
- Sensors running on **11.1 Update 1** or later releases support both SHA256 and MD5 hashes. NS-series Sensors support a maximum of 200,000 hashes for each hash type while IPS-VM600 Sensors support a maximum of 100,000 hashes for each hash type. If the Manager has both NS-series and virtual Sensors, entries over 100,000 in each hash type are pushed only to the NS-series Sensors. The push fails on virtual Sensors and a fault is raised which can be noticed in the Faults (Manager → Troubleshooting → Logs → Faults) tab.
- In case of heterogeneous environments, if the total MD5 hash entries exceed 100,000:
  - A limit exceed error can be seen in filetransfer.log during a bulk (full) update.
  - A fault will be raised in the Faults tab and error count will be incremented at the Sensor level during an incremental update. Refer to **show ab stats** command for more information.

### Note

A Full update is triggered when the total entries are more than 4000; else, an incremental update is triggered to all the Sensors connected to the Manager.

- In case MD5 and SHA256 hashes of the same file are added, the MD5 hash takes precedence over SHA256 hash of the file during analysis.

### Allow whitelisting of domains under the Sensor load

Starting with this release of 11.1, when the datapath processors on the Sensor are experiencing a high number of queued packets to be processed, the traffic from domains in the whitelist is skipped for inspection.

:

### Note about upgrading the Sensor from 10.1 to 11.1

If you are upgrading the Sensor from version 10.1 to 11.1, read the following sections carefully.

#### Interface name update in Port Throughput Usage

Starting with this release of 11.1, the Manager provides a capability to view interface name by selecting the required interface displayed at the bottom of the chart. You can access these details from Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → Performance Charts. Click Throughput tab and select Port Throughput Usage Mbps from drop-down. For any selected interface, you can view the details of Port <port number> (Interface: <interface name>), Port throughput rate in Mbps, and time in MMM DD HH:MM:SS YYYY.

This release no longer supports the following:

### Support for M-series Sensors

Starting with this release of 11.1, support to add M-series Sensors has been removed as **M-series** Sensor models have reached end of life. Users with existing M-series deployments will not be able to upgrade the Manager to 11.1 without removing these Sensors from the Manager.

### Support for 9.1 and 9.2 software

Starting with this release of 11.1, support for 9.1 and 9.2 software has been deprecated. Any deployments containing these software will not be supported.

### Note

If you plan to upgrade your deployments from 9.x to 11.1, you need to first upgrade your deployments to 10.1.7.65 (for Manager) and 10.1.5.190 (for Sensor) and then upgrade to 11.1.

### Support for XC Clusters

Starting with this release of 11.1, creation of XC Clusters has been discontinued since M-series Sensors have reached EOL.

### Configuration of Rate Limiting

Starting with this release of 11.1, Rate Limiting feature under QoS has been deprecated since M-series Sensors have reached EOL.

:

## Updating Sensor software image

Before you begin the Sensor software upgrade, make sure:

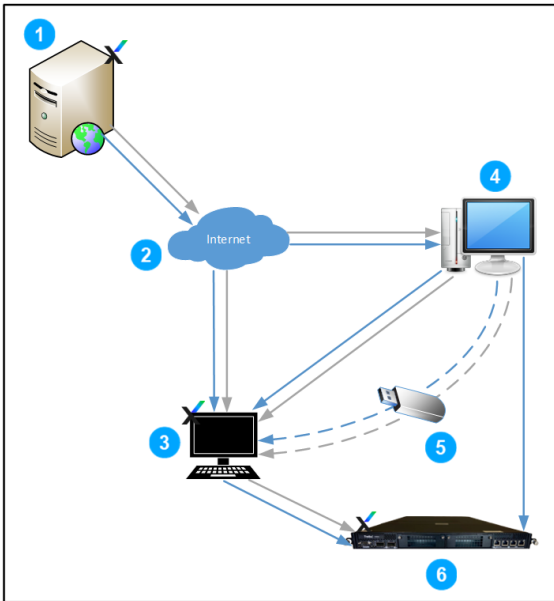
1. You have upgraded the Manager to the corresponding 11.1 version. See [Upgrading the Manager](#).
2. Your Sensors meet the requirements mentioned in [Sensor upgrade requirements](#).
3. You have understood the discussion in [Reviewing the Upgrade Considerations](#).

New Sensor software images are released periodically by Trellix and are available on Trellix IPS 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 Trellix IPS 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 Trellix IPS Update Server to any host, then import the Sensor image to the Manager server. You can then upgrade the Sensor image to the Sensor.
3. A variation of option 2: you can download the Sensor image from Trellix IPS Update Server to any host, put it on a disk, take the disk to the Manager server, and then import the image and upgrade the Sensor.
4. However, you may prefer not to upgrade the 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 upgrade the image directly to the Sensor using Sensor CLI commands. This process is described in this chapter as well.



Field	Description
1	Trellix IPS Update Server
2	Internet
3	Manager Server
4	PC/TFTP server
5	Import/disk
6	Sensor



:

### 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, Trellix recommends updating the Sensor software using the Manager for a major upgrade (for example, from 10.1 to 11.1).

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.

#### Note

Fail-open kits reduce the downtime impact of reboot considerably.

:

### Sensor software and signature set upgrade using Manager 11.1

#### Prerequisite:

You have reviewed the notes on Sensor downtime window. See [Reviewing the upgrade considerations](#).

#### Steps:

1. If you have not already done so, download the latest signature set in the Manager. In the Manager, go to Manager → <Admin Domain Name> → Trellix IPS Protection Status. Select Signature Sets tab. Then, select Download Latest Signature Set. See the *Trellix Intrusion Prevention System Product Guide*, for step-by-step information on how to download the signature set. For a list of currently supported protocols, see [KB61036](#) at [Trellix Support Portal](#). Do not push the signature set to your Sensors at this point; it will be sent with the Sensor software in step 8.

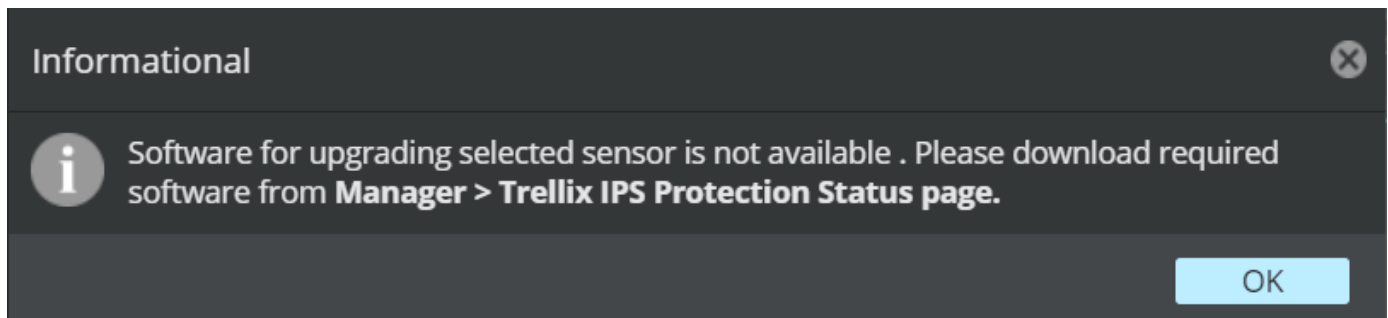
### Note

If you are using the Advanced Callback Detection feature, make sure you have downloaded the latest callback detectors to the Manager. See *Trellix Intrusion Prevention System Product Guide* for the details on downloading callback detectors.

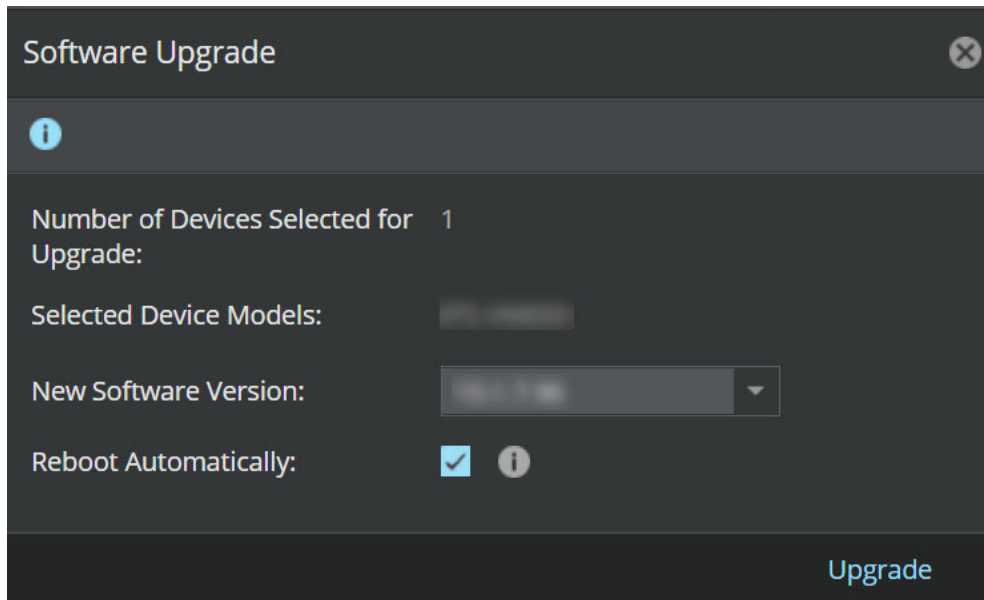
2. If you had created Trellix IPS custom attacks in the previous version of the Manager, verify that those attacks are present in the Custom Attack Editor.
3. Download the most recent 11.1 Sensor software images from the Update Server onto the Manager.
  - a. To download the Sensor software version to the Manager, go to Manager → <Admin Domain Name> → Trellix IPS Protection Status. Select Device Software tab. The Device Software tab is displayed. Select 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, go to Devices → <Admin Domain Name> → Global → Device Manager. The Device Manager page is displayed.
5. Select the Sensors tab. From the list, select the required Sensor. The Manager provides an option to concurrently perform the software upgrade for multiple Sensors using same model and software version.

### Note

For selected Sensor, if the required software version is not downloaded in the Manager, an Informational dialog box is displayed.



6. Select Upgrade Device Software from Other Actions drop-down.



The Software Upgrade dialog box is displayed.

7. Select the New Software Version to be downloaded to the Sensor from the drop-down.

### Note

You can only view the downloaded device software versions.

8. To automatically push the Sensor for reboot, enable Reboot Automatically. By default this option is enabled. If required, it can be disabled. For NS-series Sensors, you must do a full reboot as hitless reboot is not supported when SSL decryption is enabled.
9. After reboot, you need to verify the status of Sensor through CLI and confirm if it displays SIGFILE or NO\_SIGFILE. If the Sensor displays NO\_SIGFILE, manually deploy sigfile to the Sensor using Manager.
10. Click the Upgrade to initiate the process.

### Note

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 Faults tab in Manager → <Admin Domain Name> → Troubleshooting → Logs.

11. Wait for the push to complete. This process takes at least 5 minutes. To know when the process is complete, log in 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.

12. 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. To verify, go to Devices → <Admin Domain Name> → Devices → <Device Name> → Summary. Use the Performance Charts 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 Performance Charts, see *Trellix Intrusion Prevention System Product Guide*.

### Important

If you have a HA pair configured, both the Sensors forming the pair should be running on the same Sensor software version. See [Updating Sensor software in a failover pair](#).

:

## 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.

### Steps:

1. If you have not already done so, download the latest signature set. In the Manager, select Manager → <Admin Domain Name> → Trellix IPS Protection Status. Then, select Signature Sets tab. The Signature Sets tab is displayed. Select Download Latest Signature Set option. See the *Trellix Intrusion Prevention System Product Guide* for step-by-step information on how to download the signature set. For a list of currently supported protocols, see [KB61036](#) at [Trellix Support Portal](#).

### Note

If you are using the Advanced Callback Detection feature, make sure you have downloaded the latest callback detectors to the Manager. See *Trellix Intrusion Prevention System Product 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 in 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 *CLI commands* section in the *Trellix Intrusion Prevention System Product Guide*.

- c. Load the image file on the Sensor. Use the **loadimage** command as described in the *CLI commands* section in the *Trellix Intrusion Prevention System Product 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.

### Note

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 NS-series Sensors, you must do a full reboot as hitless reboot is not supported when SSL decryption is enabled. For information on these reboot options, see the *Trellix Intrusion Prevention System Product 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 Faults tab in Manager → <Admin Domain Name> → Troubleshooting → Logs.

7. After reboot, you need to verify the status of Sensor through CLI and confirm if it displays SIGFILE or NO\_SIGFILE. If the Sensor displays NO\_SIGFILE, manually deploy sigfile to the Sensor using Manager.
8. 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 HA pair

Because each Sensor in a HA pair must be rebooted after the software update, it is important to update the software in the correct order.

### Steps:

1. Push the software to each of the Sensors that are in the HA pair. You can follow one of these methods:
  - [Sensor Software and Signature Set Upgrade using Manager 11.1](#)
  - [Sensor software upgrade using a TFTP or SCP server](#).
2. Load the image file on the primary Sensor.
3. Load the image file on the secondary Sensor.

4. Reboot the primary Sensor. After reboot, you need to verify the status of Sensor through CLI and confirm if it displays SIGFILE or NO\_SIGFILE. If the Sensor displays NO\_SIGFILE, manually deploy sigfile to the Sensor using Manager.
5. Now, reboot the secondary Sensor. After reboot, you need to verify the status of Sensor through CLI and confirm if it displays SIGFILE or NO\_SIGFILE. If the Sensor displays NO\_SIGFILE, manually deploy sigfile to the Sensor using Manager. Use the Performance Charts 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 Performance Charts, see *Trellix Intrusion Prevention System Product Guide*.

:

## Uninstalling the upgrade

### Prerequisites:

- Make sure you downgrade the Sensors before you downgrade the Manager. Similarly, you must downgrade the Managers before you downgrade a Central Manager.

### Note

To downgrade Sensor software, see the relevant 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 11.1 to 10.1, then you must have the database backup from 10.1 Manager.

If the upgrade is not suitable for some reason, you can uninstall the 11.1 version and reinstall the previous version.

### Steps:

1. To uninstall an upgrade in a Windows based Manager, do the following:
  - a. 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 Trellix IPS Manager and select Stop.
  - b. Stop the Trellix IPS Manager Watchdog service using the same method as described in step 1.
  - c. Uninstall the 11.1 software that you upgraded to.
  - d. Delete the Trellix IPS Manager install directory (including the MariaDB install directory).
  - e. Reinstall the earlier version from which you upgraded.
  - f. Restore the corresponding database backup. For example, if you had downgraded from 11.1 to 10.1, then restore your 10.1 database backup.

### Note

Downgrade all Managers prior to the Central Manager downgrade.

2. To uninstall an upgrade in a Linux based Manager virtual instance, do the following:
  - a. Delete the Linux based Manager instance.
  - b. Reinstall the earlier version from which you upgraded.
  - c. Restore the corresponding database backup. For example, if you had downgraded from 11.1 to 10.1, then restore your 10.1 database backup.

### Note

Downgrade all Managers prior to the Central Manager downgrade.

3. To uninstall an upgrade in a Linux based Manager Appliance, do the following:
  - a. Obtain the bootable image of the Linux based Manager from [Trellix Support](#) for the earlier version from which you upgraded.
  - b. Reinstall the earlier version from which you upgraded on the Manager Appliance.
  - c. Restore the corresponding database backup. For example, if you had downgraded from 11.1 to 10.1, then restore your 10.1 database backup.

### Note

Downgrade all Managers prior to the Central Manager downgrade.

:

## Windows based Manager: Frequently asked questions

Here are answers to frequently asked questions.

### General

1. **Can I continue to use my Windows Server 2012 setup for 11.1 upgrade?** No. You must upgrade to one of the following supported operating systems to use Trellix IPS 11.1:
  - Windows Server 2016
  - Windows Server 2019
  - Windows Server 2022
2. **What are the available software versions of Windows-based Manager/Central Manager?** Currently, the Windows-based Manager software versions available are as follows:
  - **10.1:** 10.1.7.65, 10.1.7.66.3
  - **11.1:** 11.1.7.3.5, 11.1.7.26, 11.1.7.41, 11.1.7.71

For the list of compatible Manager and Sensor software versions, refer [Manager version and its compatible Sensor software versions](#).

### MDR

1. **In an MDR setup, after upgrading the primary Manager to 11.1, can I switch over to make the primary active or do I have to first stop the secondary?** Trellix recommends you to suspend the MDR pair, upgrade the individual Managers and then resume the MDR pair. For details, refer to [MDR Manager upgrade](#).
2. **Do I need to do any specific step after the upgrade to re-establish MDR?** No. It works automatically.
3. **After upgrading the Secondary Manager, do I need to import the database to secondary or will that happen when I re-establish MDR?** If you have suspended the MDR pair before the upgrade, the Manager will synchronize after MDR resumes.
4. **Do I need to reconfigure MDR to get primary and secondary into MDR again?** No. The MDR configuration is retained and will work automatically.
5. **In an MDR setup when will I see Switch Over and Switch Back?**
  - Switch Over: Available only when the Primary Manager is active. Clicking this will request that the Secondary Manager be active.
  - Switch Back: Available only when the Primary Manager status is in standby mode. Clicking this will switch back from the Secondary Manager and make the Primary Manager active.
6. **In an MDR setup when will I see Suspend MDR and Resume MDR?**
  - Suspend MDR: Available only on the Primary Manager when in the active state. Clicking this will instruct the Secondary Manager not to monitor via MDR Status check and to resume MDR only when indicated.
  - Resume MDR: Available only when the Primary Manager is in the suspended state. Clicking this will resume MDR mode when the MDR is suspended.

:



## COPYRIGHT

Copyright © 2024 Musarubra US LLC.

Trellix and FireEye are the trademarks or registered trademarks of Musarubra US LLC, FireEye Security Holdings US LLC and their affiliates in the US and /or other countries. McAfee is the trademark or registered trademark of McAfee LLC or its subsidiaries in the US and /or other countries. Skyhigh Security is the trademark of Skyhigh Security LLC and its affiliates in the US and other countries. Other names and brands are the property of these companies or may be claimed as the property of others.

