Trellix Intrusion Prevention System Manager Appliance Product Guide

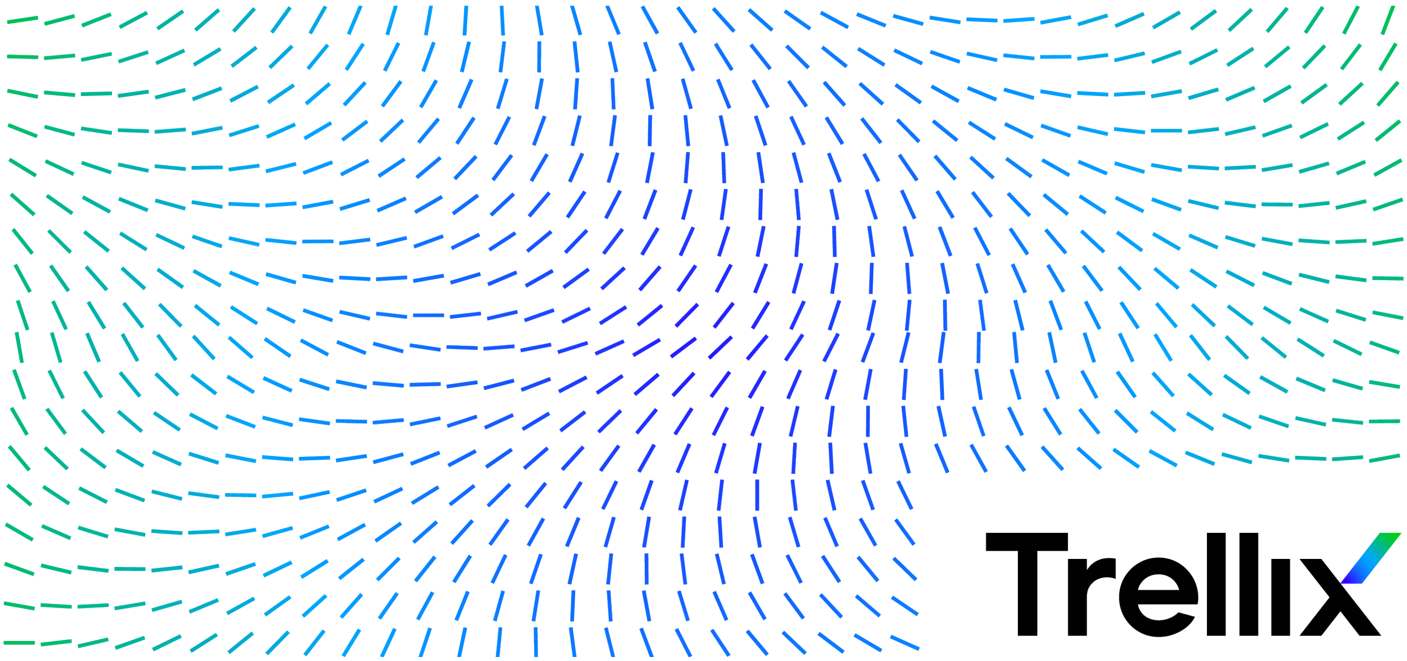


Table of Contents

Trellix Intrusion Prevention System Manager Appliance (Linux) Quick Start Guide

The Trellix Intrusion Prevention System Manager Appliance runs on a pre-installed, hardened MLOS and comes pre-loaded with the Trellix Intrusion Prevention System Manager software.

This guide provides a high-level description of how to configure the Trellix Intrusion Prevention System Manager Appliance running on MLOS. For detailed information, refer to the [Manager Appliance (Linux) Installation] section in the [Trellix Intrusion Prevention System Manager Appliance Product Guide].

Verify the shipment

Verify shipment against content list for the Accessory kit shipped with the Trellix IPS Manager Appliance.

If any of the item from the content list is missing or damaged, contact Trellix support at https://www.trellix.com/en-us/support.html.

Product documentation

Trellix Product Documentation for IPS Manager Appliance is available at the Trellix Documentation Portal.

To access the product documentation for the Manager Appliance, follow the steps below:

1. Go to Trellix Documentation Portal (https://docs.trellix.com).
2. Click **Intrusion Prevention System** from the **Network Security** tile under the **Featured Content** section.

   > **TIP**
   >
   > You can alternatively scroll down the page and click **Intrusion Prevention System** from the **Products A-Z** section.

   The **Intrusion Prevention System** documentation landing page appears displaying the list of documents categorized under various tiles.
3. Click [Manager Appliance Product Guide] from the [Hardware Guides] tile.

   Documentation for Manager Appliance opens.

Verify system specifications and requirements

These are the hardware and software specifications and requirements for the Manager Appliance.

Network recommendations

The Manager Appliance supports both DHCP and static IP address networks. Trellix strongly recommends that you use static IP address.

In addition, Trellix recommends having a DNS server on your network. This enables you to set a fully qualified domain name for your Trellix Intrusion Prevention System Manager server. The Trellix IPS Manager generates a public key certificate that uses the Manager Appliance host name. This certificate is used to authenticate the IPS Manager server to any Manager clients in your deployment.

Hardware specifications

Hardware	
Regulatory Model Name	R1000
CPU	Intel Xeon Silver 4114, 4210, or equivalent 2.20 Ghz 10C, Xeon scalable 1 per system
Hard Drive	2.5" Enterprise HDD 2 TB SATA III (6 Gbps) 7200 RPM 2 per system
DVD ROM	None
DIMM	64 GB DDR4 2133 Mhz
Integrated LAN	2 x 10 Gbe
USB ports	2 x 3.0 on front and 3 x 3.0 on rear panel
Video	DB-15 HD VGA on front and rear panel
Serial Port	RJ45 on rear panel

For information of the software specifications, refer to the sections [Server requirements] and [How to host the Manager on virtualization platforms] in the [Trellix Intrusion Prevention System Installation Guide].

Trellix recommends you to upgrade the IPS Manager software to the latest version. For more information, refer to Trellix Intrusion Prevention System 11.1.x Manager-NS-series Release Notes.

The following table lists the 10.1 Manager client requirements when using Windows 10:

	Minimum	Recommended
Operating system	Windows 10, English or Japanese **NOTE** 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	• Microsoft Edge • Mozilla Firefox • Google Chrome **NOTE** To avoid the certificate mismatch error and security warning, add the Manager web certificate to the trusted certificate list.	• Microsoft Edge 111.0 or later • Mozilla Firefox 111.0 or later • Google Chrome 111.0 or later

The following are Manager client requirements when using Mac:

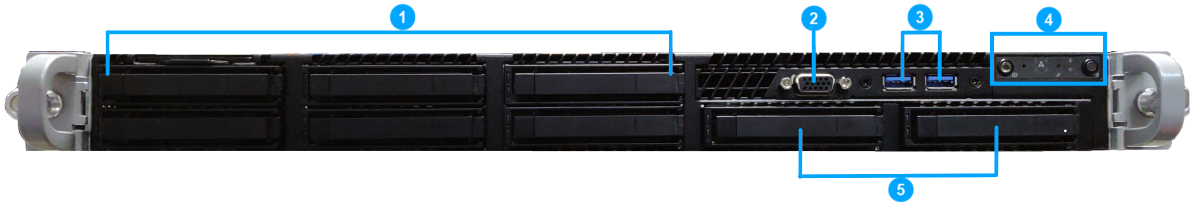
Mac operating system	Browser
Ventura	Safari 16 or later

Manager Appliance front panel description

The Manager Appliance front panel contains ports, LED lights for status and buttons to perform operations.

An optional lockable bezel is included with the Manager Appliance which can be installed to cover the front panel.

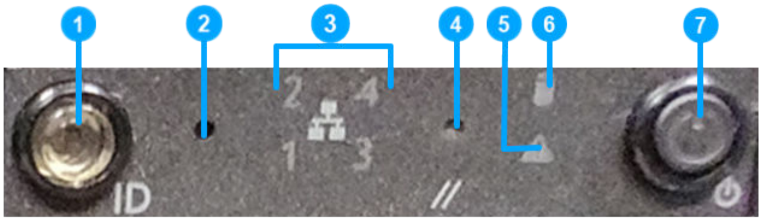
Figure 1. Manager Appliance Front Panel



Item	Description
1	Drive bay (1, 2, 3, 4, 5, 6) configuration
2	Console port

Item	Description
3	USB ports
4	Front control panel
5	Drive bay (7, 8) configuration

Figure 2. Front Control Panel

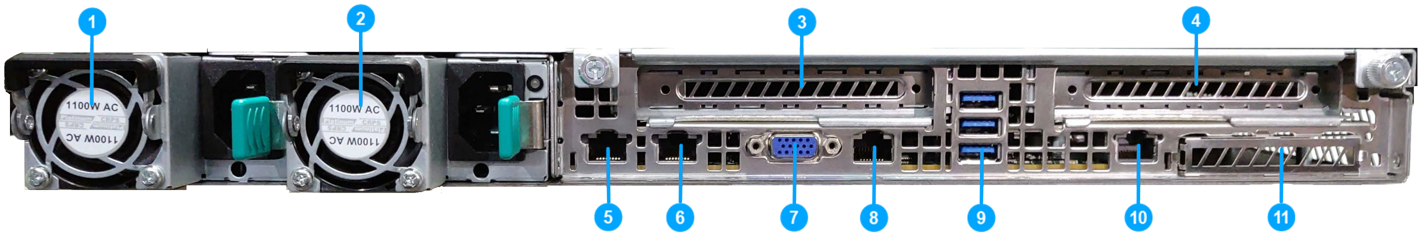


Item	Description
1	System ID button integrated with LED
2	Non-maskable interrupt (NMI) button
3	Port activity LEDs: 1. NIC 1 2. NIC 2 3. Serial Port 4. Management Port
4	System Cold Reset Button
5	System status LED
6	Drive activity LED
7	Power button integrated with LED

Manager Appliance back panel description

The Manager Appliance back panel contains ports and connectors for configuration.

Figure 3. Manager Appliance Back Panel



Item	Description
1	Power supply 1
2	Power supply 2
3	PCIe* Riser 1
4	PCIe* Riser 2
5	NIC 1 connector RJ-45
6	NIC 2 connector RJ-45
7	Console port
8	Serial port connector RJ-45
9	USB ports
10	Management port
11	OCP module bay

Manager Appliance LEDs

The front panel LEDs provide status information for the health of the Manager Appliance and the activity on its ports. The following table describes the MLOS Manager Appliance LEDs.

LED	Status	Description
System ID **NOTE** Initially, you should press the System ID button to see the status.	Solid Blue	Functioning
	Off	Not functioning
NIC Activity	Solid Green	Network Interface Controller (NIC) has detected a network link.
	Blinking Green	Network link is up and healthy.
	Off	Network Interface Controller (NIC) has not detected any network link.
System Status	Solid Green	Operating in good health
	Blinking Green	Operating in redundant state
	Solid Amber	Non-recoverable halt state
	Blinking Amber	Operating in critical health and indicates an expected failure warning
	Off	Not operating
Drive activity	Solid Green	Manager Appliance has identified an external drive in the system.
	Off	Manager Appliance has not identified any external drive.

LED	Status	Description
Power	Solid Green	Manager Appliance has power feed.
	Off	Manager Appliance has no power feed.
Power Supply 1	Solid Green	Power supply unit has power feed and is functioning.
	Blinking Green	Power supply unit has power feed and is redundant.
	Red	Power supply unit has no power feed or is not functioning.
	Off	Manager Appliance has no power feed.
Power Supply 2	Solid Green	Power supply unit has power feed and is functioning.
	Blinking Green	Power supply unit has power feed and is redundant.
	Red	Power supply unit has no power feed or is not functioning.
	Off	Manager Appliance has no power feed.

Rack installation

The following steps explain the procedure to install the rack for the Manager Appliance.

NOTE

For graphical representation of the rack installation, refer to the [Rail Kit Installation Guide] shipped with the appliance box.

1. Identify the Right (R) and Left (L) Rail Assemblies.
2. Extend each rail assembly to expose the stamped 'R' and 'L' identifiers.
3. Install left rail assembly.

   NOTE

   Use mounting holes within the same 1U space on both front and rear rack pillars.

4. The rail is securely installed when the hook and locker that extends out of the mounting hole are fully sealed and locked into place.
5. Repeat steps b - d for right rail assembly.
6. When transporting the rack with systems pre-installed, the 10-32 shipping screws must be screwed to the center hole of the rear rail bracket to prevent possible rail mounting failure.

Server system installation

Carefully install the Manager Appliance on the mounting rails.

NOTE

For graphical representation of the server system installation, refer to the [Rail Kit Installation Guide] shipped with the appliance box.

Steps:

1. Fully extend the rails until they lock in place.
2. Align and insert rear mounting posts of the server into rear mounting slots of both rails.
3. Carefully rotate server down until the remaining two server mounting posts on each side of the chassis install into the mounting slots of each rail.
4. Verify that the server lock is fully engaged and the system is fully sealed into each rail.

Install system into rack

These steps explain the procedure to install the Manager Appliance into the rack.

NOTE

For graphical representation, refer to the [Rail Kit Installation Guide] shipped with the appliance box.

1. Lift the release tab of both rails.
2. Push the appliance as far as possible into the rack.
3. Use the fixed locking screws located on the system rack handles to secure the system to the rack.

Connect the Manager Appliance to power supply and network

After you have installed the Manager Appliance on the rack, connect the appliance to the power source and to your network. Connect a monitor, keyboard, and a mouse, which are needed to configure the Manager Appliance.

Perform the following steps to connect the Manager Appliance to a power source and network.

1. Plug the AC power cord to the power supply slot located in the back panel of the Manager Appliance, then plug the other end of the cord into an appropriate power source.
2. Connect network cables to the NIC ports.

   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.

3. Connect the monitor, mouse, and keyboard to the rear or front of the Manager Appliance.

NOTE

You can manage the Manager Appliance from a remote computer using SSH after the initial installation and configuration is completed.

4. Turn on the power for the Manager Appliance.

CAUTION

Appliance power on/off — the push-button on/off power switch on the front panel of the Manager Appliance does not turn off the AC power. To remove AC power from the Manager Appliance, you must unplug the AC power cord from either the power supply or wall outlet.

5. Wait for the appliance to start and login with a valid username and password.
6. Go to Configure the Manager Appliance (page 11) for default user credentials and steps to configure the Manager Appliance.

Configure the Manager Appliance

Log in to the Manager Appliance using a console client and configure the network settings as shown below.

1. Log in to the Manager shell using the following credentials:
   - Username: **`admin`**
   - Password: **`MLOSnsmApp`**

   NOTE

   SSH connection to the Linux based Manager Appliance is not supported by Putty application. Trellix recommends you to use Tera Term application for remote access to 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 the 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 Linux 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
`DOMAIN NAME`	Enter the domain name for the Manager server.
`HOSTNAME`	Enter the hostname to be assigned to the Manager server.
`Configuring the eth"x" with public IP`	
`IP ADDRESS`	Enter the public IP address to be assigned to the Manager server.
`NETMASK`	Enter the subnet mask for the Manager server.
`GATEWAY`	Enter the gateway address for the Manager server.
`DNS1`	Enter the primary DNS server IP address.
`Do you want to enter DNS2 <y/n>`	Type **`y`**, if you want to configure a secondary DNS server IP address, else type **`n`**.
`DNS2`	(Optional) Enter the secondary DNS server IP address.
`Configuring the eth"y" with private IP` (Applicable only when **`2 -> Configure Both the NIC's`** option is selected in step a).	
`IP ADDRESS`	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

The Manager GUI can be accessed using the public IP address assigned to the Manager server.

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.

Commands for the Manager service

To check the status of the Manager, execute the **`manager status`** command.

To start the Manager, execute the **`manager start`** command.

To stop the Manager, execute the **`manager stop`** command.

Access Manager UI from a client machine

You can manage the application remotely by accessing the UI of Manager using a client computer.

Steps:

1. Start your browser and then type the following URL of the Manager Appliance:

   `https://<hostname.domainname or host-IP>`

2. For initial login after a new installation:

   For Login ID, type **`admin`**

   For Password, type **`admin123`**

   > **NOTE**
   >
   > Trellix strongly recommends that you change the default username and password after the first login to the Manager.

Manager Appliance (Linux) Installation

About the Trellix Intrusion Prevention System Manager Appliance

The Trellix Intrusion Prevention System Manager Appliance is part of the Trellix Intrusion Prevention System. The Manager Appliance is a 1-U rack dense chassis with multi-core Intel XEON Series Processor and four 2.5" hard drive trays.

The Trellix Intrusion Prevention System Manager Appliance runs on a pre-installed, hardened MLOS and comes pre-loaded with the Trellix Intrusion Prevention System Manager software.

Warnings and cautions

You should be aware of these warning and cautions.

⚠ **CAUTION**

Trellix IPS Manager Appliance power on or off — the push button On/Off power switch on the front panel of the Manager Appliance does not turn off the AC power. To remove AC power from the IPS Manager Appliance, you must unplug the AC power cord from either the power supply or wall outlet.

⚠ **CAUTION**

The power supplies in your system might produce high voltages and energy hazards, which can cause bodily harm. Only trained service technicians are authorized to remove the covers and access any of the components inside the system.

⚠ **CAUTION**

This system may have more than one power supply cable. To reduce the risk of electrical shock, only a trained service technician must disconnect all power supply cables before servicing the system.

⚠ **CAUTION**

Hazardous conditions — devices and cables: Hazardous electrical conditions may be present on power, telephone, and communication cables. Turn off the Manager Appliance and disconnect telecommunications systems, networks, modems, and the power cord attached to the Manager Appliance before opening it. Otherwise, personal injury or equipment damage can result.

⚠ **CAUTION**

Avoid injury — lifting the Manager Appliance and attaching it to the rack is a two-person job. The Manager Appliance weighs approximately 10.46 kg (23.05 lbs).

Before installing the Manager Appliance

Make sure to check for the following before you install the Manager Appliance.

- Read all provided safety information.
- Make sure that you have selected a suitable location for installing the Manager Appliance.
- Check that you have all the necessary equipment and components outlined in this document.
- Familiarize yourself with the Manager Appliance network access card (NIC) ports and connectors as described in this document.
- Decide whether you will be using static or dynamic IP address assignment. If you use a static IP address for the Manager Appliance, you must request a static IP address from your network administrator, who must then update your DNS server with a valid Manager Appliance host name entry. You must have the following information available when you configure the Manager Appliance:
  - Static IP address
  - Network mask
  - Default gateway address
  - A primary and an optional secondary DNS server IP address

> ⚠ **CAUTION**
>
> To ensure the safe operation of the Manager Appliance, read all documentation before installation.

System specifications and environmental requests

These are the system specifications and requirements for the Manager Appliance.

Network recommendations

Although the Manager Appliance supports both DHCP and static IP address networks, Trellix strongly recommends that you use static IP addresses.

In addition, Trellix recommends having a DNS server on your network. This enables you to set a fully qualified domain name for your Trellix Intrusion Prevention System Manager server. The Trellix IPS Manager generates a public key certificate that uses the Manager Appliance host name. This certificate is used to authenticate the IPS Manager server to any Manager clients in your deployment.

Table 1. Hardware and Software specifications

Component	Specifications
Hardware	
Regulatory Model Name	R1000
CPU	Intel Xeon Silver 4114, 4210, or equivalent, 2.20 Ghz, 10C, Xeon scalable, 1 per system

Component	Specifications
Hard Drive	2.5" Enterprise HDD2TBSATA III (6Gbps)7200 RPM2 per system
DVD ROM	None
DIMM	64GB DDR42133Mhz
Integrated LAN	2 x 10 Gbe
USB ports	2 x 3.0 on front and 3 x 3.0 on rear panel
Video	DB-15 HD VGA on front & rear panel
Serial Port	RJ45 on rear panel

For information of the software specifications, refer to the sections [Server requirements] and [How to host the Manager on virtualization platforms] in the [Trellix Intrusion Prevention System Installation Guide].

NOTE

Trellix recommends you to upgrade the IPS Manager software to the latest version. For more information, refer to Trellix Intrusion Prevention System 11.1.x Manager-NS-series Release Notes.

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 **NOTE** 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	• Microsoft Edge • Mozilla Firefox • Google Chrome **NOTE** To avoid the certificate mismatch error and security warning, add the Manager web certificate to the trusted certificate list.	• Microsoft Edge 111.0 or later • Mozilla Firefox 111.0 or later • Google Chrome 111.0 or later

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

Mac operating system	Browser
Ventura	Safari 16 or later

NOTE

Manager Appliance supports only USB-compliant mouse and keyboard (PS/2 mouse and keyboard are not supported).

Features not supported

- User interface support on Appliance
- Vulnerability Manager support
- Localization

Verify the shipment

Verify shipment against content list for the Accessory kit shipped with the Manager Appliance.

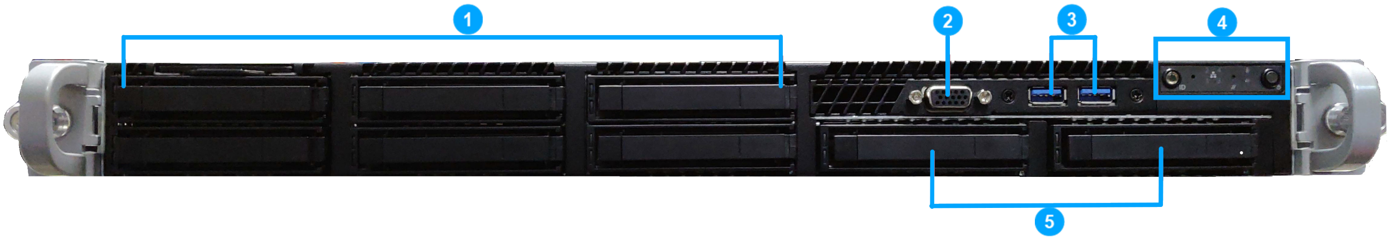
If any of the content from the content list is missing or damaged, contact Trellix support at https://www.Trellix.com/en-us/support.html.

Manager Appliance front panel description

The Manager Appliance front panel contains ports, LED lights for status and buttons to perform operations.

An optional lockable bezel is included with the Manager Appliance, which can be installed to cover the front panel.

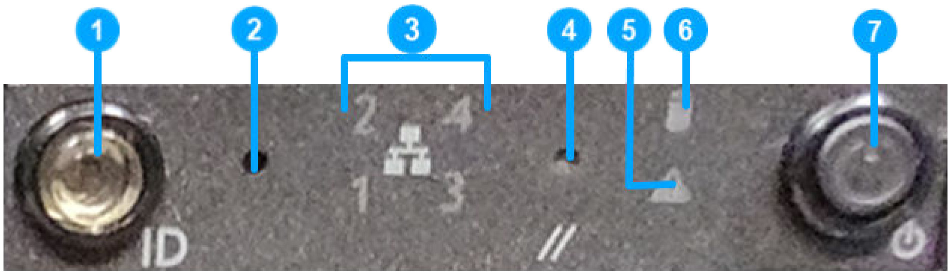
Figure 4. Manager Appliance Front Panel



Item	Description
1	Drive bay (1, 2, 3, 4, 5, 6) configuration
2	Console port
3	USB ports
4	Front control panel

Item	Description
5	Drive bay (7, 8) configuration

Figure 5. Front Control Panel

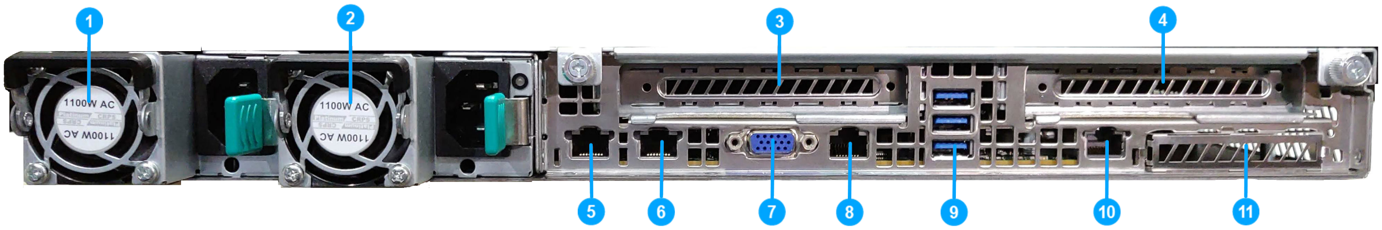


Item	Description
1	System ID button integrated with LED
2	Non-maskable interrupt (NMI) button
3	Port activity LEDs: 1. NIC 1 2. NIC 2 3. Serial Port 4. Management Port
4	System Cold Reset Button
5	System status LED
6	Drive activity LED
7	Power button integrated with LED

Manager Appliance back panel description

The Manager Appliance back panel has these ports and connectors for configuration.

Figure 6. Manager Appliance Back Panel



Item	Description
1	Power supply 1
2	Power supply 2
3	PCIe* Riser 1
4	PCIe* Riser 2
5	NIC 1 connector RJ-45
6	NIC 2 connector RJ-45
7	Console port
8	Serial port connector RJ-45
9	USB ports
10	Management port
11	OCP module bay

Manager Appliance LEDs

The front panel LEDs provide status information for the health of the Manager Appliance and the activity on its ports. The following table describes the MLOS Manager Appliance LEDs.

LED	Status	Description
System ID **NOTE** Initially, you should press the System ID button to see the status.	Solid Blue	Functioning
	Off	Not functioning
NIC Activity	Solid Green	Network Interface Controller (NIC) has detected a network link.
	Blinking Green	Network link is up and healthy.
	Off	Network Interface Controller (NIC) has not detected any network link.
System Status	Solid Green	Operating in good health
	Blinking Green	Operating in redundant state
	Solid Amber	Non-recoverable halt state
	Blinking Amber	Operating in critical health and indicates an expected failure warning
	Off	Not operating
Drive activity	Solid Green	Manager Appliance has identified an external drive in the system.
	Off	Manager Appliance has not identified any external drive.

LED	Status	Description
Power	Solid Green	Manager Appliance has power feed.
	Off	Manager Appliance has no power feed.
Power Supply 1	Solid Green	Power supply unit has power feed and is functioning.
	Blinking Green	Power supply unit has power feed and is redundant.
	Red	Power supply unit has no power feed or is not functioning.
	Off	Manager Appliance has no power feed.
Power Supply 2	Solid Green	Power supply unit has power feed and is functioning.
	Blinking Green	Power supply unit has power feed and is redundant.
	Red	Power supply unit has no power feed or is not functioning.
	Off	Manager Appliance has no power feed.

Installing the Manager Appliance

This section describes how to attach rails and mount the Manager Appliance on a rack.

A rack mounting kit is supplied with the Manager Appliance so you can install the Manager Appliance in a 19-inch rack, as described in the following rack mounting instructions.

The rack mounting contains:

- Slide rails
- Chassis cable management arm

> **NOTE**
>
> A screwdriver is required for this procedure.

Positioning the Manager Appliance

The Manager Appliance must be installed in a suitable location. Since it is designed to be operated remotely, physical access to the Manager Appliance is needed only to connect networking cables and the power supply cord, a monitor, keyboard, and mouse to configure the software.

Initial setup requires attaching a single network cable to the back of the Manager Appliance. After the network setup is finished, physical access to the Manager Appliance is necessary only to restart the appliance. Trellix recommends that you interact with the system using remote desktop software.

Rack installation

These steps explain the procedure to install the rack for the Manager Appliance.

NOTE

For graphical representation of the rack installation, refer to the [Rail Kit Installation Guide] shipped with the appliance box.

1. Identify the Right (R) and Left (L) Rail Assemblies.
2. Extend each rail assembly to expose the stamped 'R' and 'L' identifiers.
3. Install left rail assembly.

   NOTE

   Use mounting holes within the same 1U space on both front and rear rack pillars.

   The rail is securely installed when the hook and locker that extends out of the mounting hole are fully sealed and locked into place.
4. Repeat steps 2 - 3 for right rail assembly.

   NOTE

   When transporting the rack with systems pre-installed, the 10-32 shipping screws must be screwed to the center hole of the rear rail bracket to prevent possible rail mounting failure.

Server system installation

Carefully install the Manager Appliance on the mounting rails.

NOTE

For graphical representation of the server system installation, refer to the [Rail Kit Installation Guide] shipped with the appliance box.

Steps:

1. Fully extend the rails until they lock in place.
2. Align and insert rear mounting posts of the server into rear mounting slots of both rails.
3. Carefully rotate server down until the remaining two server mounting posts on each side of the chassis install into the mounting slots of each rail.
4. Verify that the server lock is fully engaged and the system is fully sealed into each rail.

Install system into rack

These steps explain the procedure to install the Manager Appliance into the rack.

NOTE

For graphical representation, refer to the [Rail Kit Installation Guide] shipped with the appliance box.

1. Lift the release tab of both rails.
2. Push the appliance as far as possible into the rack.
3. Use the fixed locking screws located on the system rack handles to secure the system to the rack.

Remove the Manager Appliance from the rails

Perform these steps to remove the Manager Appliance.

1. Turn off the Manager Appliance and disconnect it from the power outlet.
2. Disconnect all cables, such as network cables. Disconnect the monitor, keyboard, and mouse cables as well, if installed.
3. If installed, remove screws securing the appliance to the rack mount rails.
4. Pull the appliance out of the rack until the safety catches stop the movement.
5. Rotate the release latch at the front of each rail to disengage the safety catch.
6. With help from another person, lift the system completely out of the rack.

Configuring the Manager Appliance

The Manager Appliance comes with all Manager components pre-installed. The Manager Appliance Configuration Tool configures the Manager Appliance and starts as soon as you log on to the Manager Appliance.

Connect the Manager Appliance to power and the network

After you have fixed the Manager Appliance on the rack, connect the appliance to the power source and to your network. Connect a monitor, keyboard, and a mouse, which are required to configure the Manager Appliance.

Perform the following steps to connect the Manager Appliance to a power source and network.

1. Plug the AC power cord to the power supply slot located in the back panel of the Manager Appliance, then plug the other end of the cord into an appropriate power source.
2. Connect network cables to the NIC ports.

   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.

3. Connect the monitor, mouse, and keyboard to the rear or front of the Manager Appliance.

NOTE

You can manage the Manager Appliance from a remote computer using SSH after the initial installation and configuration is completed.

4. Turn on the power for the Manager Appliance.

CAUTION

Appliance power on/off — the push-button on/off power switch on the front panel of the Manager Appliance does not turn off the AC power. To remove AC power from the Manager Appliance, you must unplug the AC power cord from either the power supply or wall outlet.

5. Wait for the appliance to start and login with a valid username and password.
6. Go to Configure the Manager Appliance (page 25) for default user credentials and steps to configure the Manager Appliance.

Dual NIC support in Linux based Manager

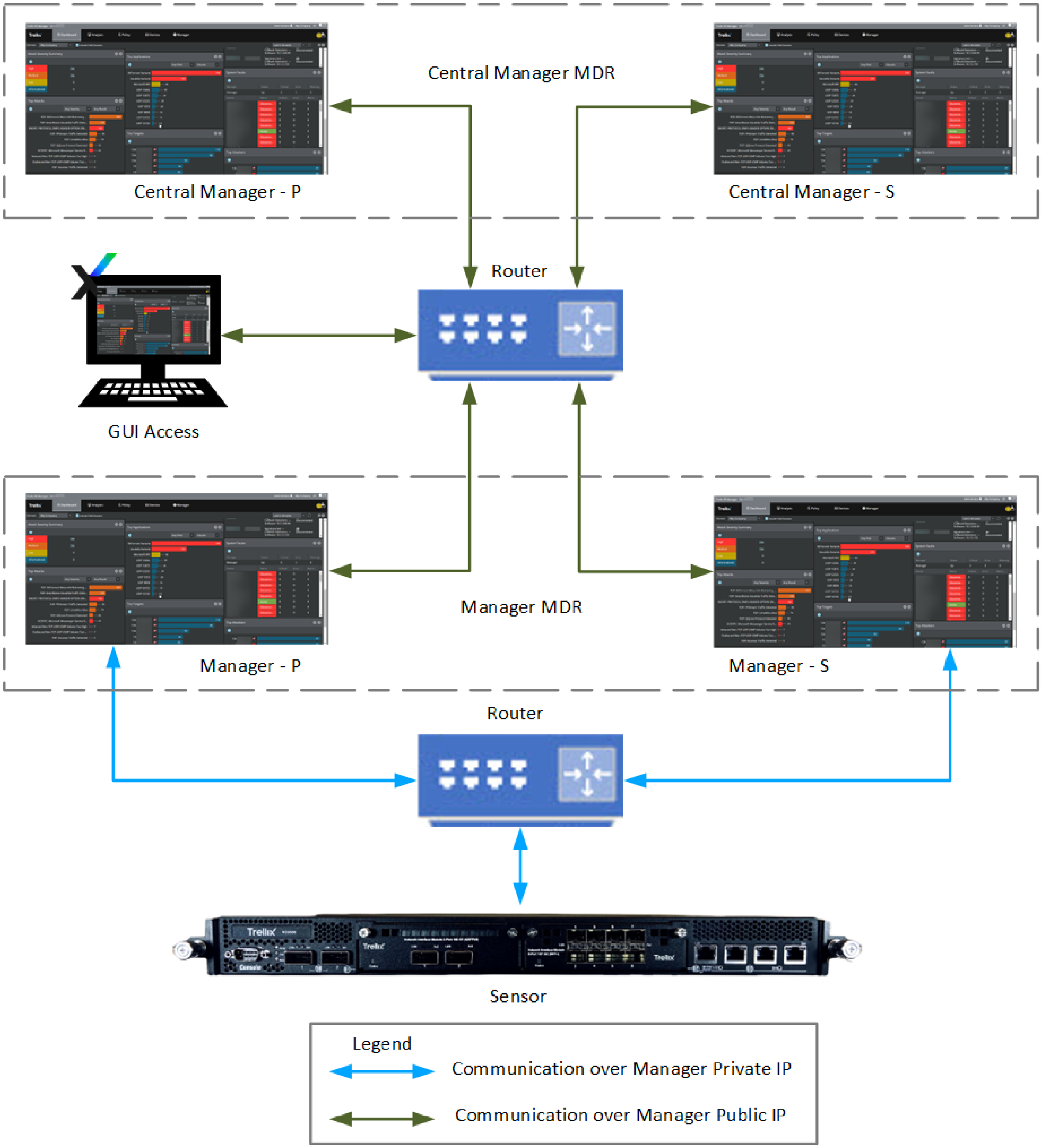
The Linux based Manager supports dual NIC. It means you can configure both public and private IP addresses to the Linux based Manager.

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.

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 Appliance

Log in to the Manager Appliance using a console client and configure the network settings as shown below.

1. Log in to the Manager shell using the following credentials:
    - Username: **`admin`**

- Password: **`MLOSnsmApp`**

> **NOTE**
>
> SSH connection to the Linux based Manager Appliance is not supported by Putty application. Trellix recommends you to use Tera Term application for remote access to 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 the 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
`DOMAIN NAME`	Enter the domain name for the Manager server.
`HOSTNAME`	Enter the hostname to be assigned to the Manager server.
`Configuring the eth"x" with public IP`	
`IP ADDRESS`	Enter the public IP address to be assigned to the Manager server.
`NETMASK`	Enter the subnet mask for the Manager server.
`GATEWAY`	Enter the gateway address for the Manager server.
`DNS1`	Enter the primary DNS server IP address.
`Do you want to enter DNS2 <y/n>`	Type **`y`**, if you want to configure a secondary DNS server IP address, else type **`n`**.
`DNS2`	(Optional) Enter the secondary DNS server IP address.
`Configuring the eth"y" with private IP` (Applicable only when **`2 -> Configure Both the NIC's`** option is selected in step a).	
`IP ADDRESS`	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

The Manager GUI can be accessed using the public IP address assigned to the Manager server.

> **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.

SSH public key based authentication for Manager Appliance (Linux)

You can use SSH public key authentication or password based authentication to login to the Manager or the remote machine using SSH. Use of public key authentication allows administrators and users to access the Manager or the remote machine without the use of password based authentication.

Manager as the SSH client

When the Manager serves as the SSH client, you can SCP files to a remote machine serving as a SCP server from the Manager. This requires the SSH public key generated on the Manager to be configured on the remote SCP server. The Manager uploads the key to the remote SCP sever. Perform the following steps to access the SCP server on a remote machine from the Manager:

1. Login to the Manager appliance with the username and password.
2. Execute the **`publicKeyAuth`** command .
3. Choose **`Upload Key To A Server`** and press **`Enter`**.
4. Enter the SCP server IP address.
5. Enter the SCP server username.
6. Enter the SCP server password to transfer the public key to the remote machine.

   The public key is successfully uploaded to the remote machine.
7. To check if the key is uploaded, try logging into the machine, with **`ssh <username>@<SCP server IP address>.`**

   The SSH public key based authentication is successful.

Sample output

```
MLOS-78> publicKeyAuth

Choose one of the below options

1: Upload Key To A Server

2: Download Key From Client

Input [1] or [2] : 1

[sudo] password for admin:

Please provide with the following inputs.

[Thu Feb 20 10:57:44 UTC 2020] : Enter The SCP Server IP : 10.1.1.1

[Thu Feb 20 10:57:44 UTC 2020] : Enter SCP Server UserName : admin

[Thu Feb 20 10:57:44 UTC 2020] : Checking if .ssh/ already exists.
```

```
[Thu Feb 20 10:57:44 UTC 2020] : The /home/admin/.ssh already exists!
[Thu Feb 20 10:57:44 UTC 2020] : Checking if public key already exists.
[Thu Feb 20 10:57:44 UTC 2020] : The /home/admin/.ssh/id_ecdsa.pub does not exists!
[Thu Feb 20 10:57:44 UTC 2020] : Creating a key pair.
Generating public/private ecdsa key pair.
Your identification has been saved in /home/admin/.ssh/id_ecdsa.
Your public key has been saved in /home/admin/.ssh/id_ecdsa.pub.
The key fingerprint is:
SHA256:7M1msETM8MRYZGqNnRDx+OV/anEOCQfxcbAUe2q+Dno admin@MLOS-78
The key's randomart image is:
+---[ECDSA 256]---+
| +B+ ..=o.|
| oXo..o = |
|=*= ..+ .|
|. .=+. .o |
|.o So...|
| .o. .+o. |
|..o. .=+ .|
|. o..+E+ |
| o..o. .|
+----[SHA256]-----+
[Thu Feb 20 10:57:44 UTC 2020] : Successfully created the key pair.
[Thu Feb 20 10:57:44 UTC 2020] : Changing permissions of local .ssh/ dir
[Thu Feb 20 10:57:44 UTC 2020] : Successfully changed the permissions of the dir/file to 700
[Thu Feb 20 10:57:44 UTC 2020] : Transfering public key to remote machine. The operation might ask for password.
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/admin/.ssh/id_ecdsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
```

```
FIPS mode initialized

admin@10.1.1.1's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'admin@10.1.1.1'"

and check to make sure that only the key(s) you wanted were added.

[Thu Feb 20 10:57:44 UTC 2020] : Successfully copied the key to 10.1.1.1

[Thu Feb 20 10:57:44 UTC 2020] : Modifying .ssh/ related dir/file permissions on the remote machine.
The operation might ask for password.

FIPS mode initialized

[Thu Feb 20 10:57:44 UTC 2020] : Successfully modified the permissions of .ssh/authorized_keys on
remote machine.
```

Manager as the SSH server

When the Manager serves as the SSH server, you can SCP files from a remote machine serving as a SCP client to the Manager. This requires the SSH public key generated on the remote SCP client to be configured on the Manager. The Manager downloads the key from the remote SCP client. Perform the following steps to access the Manager from the SCP client on a remote machine:

1. Login to the Manager appliance with the username and password.
2. Execute the **`publicKeyAuth`** command.
3. Choose **`Download Key From Client`** and press **`Enter`**.
4. Enter the SCP client IP address.
5. Enter the SCP client username.
6. Enter the public key file location given on the SCP client machine.
7. Enter the SCP client password to transfer the public key to the remote machine.

   The public key is successfully downloaded from the remote machine. The SSH public key based authentication is successful.

Sample output

```
MLOS-78> publicKeyAuth

Choose one of the below options

1: Upload Key To A Server

2: Download Key From Client

Input [1] or [2] : 2

[sudo] password for admin:

Please provide with the following inputs.

[Thu Feb 20 10:51:14 UTC 2020] : Enter The SCP Client IP : 10.1.1.1
```

```
[Thu Feb 20 10:51:14 UTC 2020] : Enter SCP Client UserName : admin

[NOTE] : Please Make Sure The Public Key Is Generated Using ECDSA

[Thu Feb 20 10:51:14 UTC 2020] : Public Key File Location On Client : /home/admin/.ssh/id_ecdsa.pub

[Thu Feb 20 10:51:14 UTC 2020] : The /home/admin/.ssh already exists!

[Thu Feb 20 10:51:14 UTC 2020] : Changing permissions of local .ssh/ dir

[Thu Feb 20 10:51:14 UTC 2020] : Successfully changed the permissions of the dir/file to 700

[Thu Feb 20 10:51:14 UTC 2020] : Downloading Public Key from Client : 10.1.1.1 to Server

FIPS mode initialized

admin@10.1.1.1's password:

id_ecdsa.pub 100% 177 326.2KB/s 00:00

[Thu Feb 20 10:51:14 UTC 2020] : Validating Public Key Algorithm

Download Successful

[Thu Feb 20 10:51:14 UTC 2020] : Resetting the permissions of the file .ssh/authorized_keys on local
machine

[Thu Feb 20 10:51:14 UTC 2020] : Successfully modified the permissions of .ssh/authorized_keys on
remote machine.
```

Reconfiguration of SSH and SSHD

During the Manager installation, configurational scripts are run automatically to harden the operating system as a best practice.

Reconfiguration of SSH

After the configuration scripts are run, the SSH configuration file contains the following configuration:

Configuration	Comments
Protocol 2	Use of protocol version 1 is not recommended. It may be susceptible to man-in-the-middle attacks.
Ciphers • AES: aes256-gcm@openssh.com, aes128-gcm@openssh.com • MAC: hmac-sha2-256, and hmac-sha2-512 • KexAlgorithms: ecdh-sha2-nistp256	Use of strong cipher suites to make the encryptions better. The MAC (Message Authentication Code) algorithm is used in protocol version 2 for data integrity protection. Multiple algorithms must be comma-separated.

Reconfiguration of SSHD

After the configuration scripts are run, the SSHD configuration file contains the following configuration:

Configuration	Comments
Port 22	Used for SSH communication
Protocol 2	Use of protocol version 1 is not recommended. It may be susceptible to man-in-the-middle attacks.
HostKey /etc/ssh/ssh_host_dsa_key	Specifies a file containing a private host key used by SSH
RekeyLimit 1G 1h	The first argument specifies the maximum amount of data that can be transmitted before the session key is renegotiated. The second argument, which is optional, specifies the maximum amount of time that may pass before the session key is renegotiated. The first argument is specified in bytes and may have a suffix of K, M, or G to indicate Kilobytes, Megabytes, or Gigabytes, respectively.
SyslogFacility AUTH	Specifies the facility code that is used when logging messages from sshd. The default value is AUTH
LogLevel VERBOSE	Specifies the verbosity level that is used when logging messages from sshd
Ciphers • AES: aes256-gcm@openssh.com, aes128-gcm@openssh.com • MAC: hmac-sha2-256, and hmac-sha2-512 • KexAlgorithms: ecdh-sha2-nistp256 • HostKeyAlgorithms: ecdsa-sha2-nistp256	Use of strong cipher suites to make the encryptions better. The MAC (Message Authentication Code) algorithm is used in protocol version 2 for data integrity protection. Multiple algorithms must be comma-separated.
LoginGraceTime 300	Specifies the time limit after which the server disconnects if the user is not successfully logged in
PermitRootLogin no	Specifies whether the root user can log in using ssh. The default value is **yes**.
StrictModes yes	Specifies whether sshd should check file modes and ownership of the user's files and home directory before accepting login. The default value is **no**.
MaxAuthTries 3	Specifies the maximum number of authentication attempts permitted per connection
HostbasedAuthentication no	Specifies whether rhosts or `/etc/hosts.equiv` authentication together with successful public key client host authentication is allowed.
IgnoreUserKnownHosts yes	Specifies whether sshd should ignore the user's `~/.ssh/known_hosts` during RhostsRSAAuthentication or HostbasedAuthentication
AllowAgentForwarding no	Specifies whether ssh-agent forwarding is permitted
AllowTcpForwarding no	Specifies whether TCP forwarding is permitted
X11Forwarding no	Specifies whether X11 forwarding is permitted
PrintMotd yes	Specifies whether sshd should print `/etc/motd` when a user logs in interactively

Configuration	Comments
TCPKeepAlive yes	Specifies whether the system should send TCP keepalive messages to the other side. The default is **yes** (to send TCP keepalive messages), and the server will notice if the network goes down or the client host crashes. This avoids infinitely hanging sessions.
MaxStartups 3	Specifies the maximum number of concurrent unauthenticated connections to the SSH daemon. Additional connections will be dropped until authentication succeeds or the LoginGraceTime expires for a connection.
Banner /etc/legal	The contents of the specified file are sent to the remote user before authentication is allowed.
Subsystem sftp /usr/libexec/sftp-server (modified from Subsystem sftp /usr/libexec/openssh/sftp-server)	Configures an external subsystem, such as a file transfer daemon. Arguments should be a subsystem name and a command to execute upon subsystem request. The sftp-server command implements the SFTP file transfer subsystem.
User authentication	Password, ssh-rsa, rsa-sha2-256, rsa-sha2-512 and ecdsa-sha2-nistp256.

Commands for the Manager service

To check the status of the Manager, execute the **`manager status`** command.

To start the Manager, execute the **`manager start`** command.

To stop the Manager, execute the **`manager stop`** command.

Working with the Manager software

After the configuration, you can access the Manager software from a client system using a supported browser.

For information on using the Manager software, refer to the [Manager Administration] section in [Trellix Intrusion Prevention System Product Guide].

Access the Manager from a client machine

You can access the Manager Appliance's user interface from a client machine.

- Start your browser and then type the URL of the Manager Appliance:

  ```
  https://<hostname.domainname or host-IP>
  ```

Login to the Manager

After you successfully install and configure the Manager, the **Login Screen** appears when you access the Manager user interface through a browser.

1. Do one of the following:

   For initial login after a new installation:

   - For **Login ID**, type `admin`.

     NOTE

     In case of the Trellix IPS Central Manager, the **Login ID** is `nscmadmin`.

   - For **Password**, type `admin123`.

     TIP

     Trellix strongly recommends that you change the default username and password in the Manager. For more information about the Manager application, see the [Trellix Intrusion Prevention System Product Guide].

   If you are not the Trellix IPS system administrator/Super User:

   - Type the **Login ID** supplied to you by your administrator.
   - Type the valid **Password** for the specified Login ID.

2. Click **Login** or press **Enter**. The Manager Dashboard page appears.

Maintaining the Manager Appliance

The Manager Appliance requires some user interaction for optimal performance.

This interaction involves regular monitoring and maintenance of the environment, including the Manager Appliance hardware, Microsoft Windows operating system, updates to the Manager software application including the embedded database, Trellix Anti-Virus software, and Manager Appliance security hardening posture.

Upgrading your Manager software

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 IPS 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 software are upgraded simultaneously.

Prerequisites:

1. Make sure you have a Linux machine installed in your network.
2. You must download the Manager upgrade file (setup.bin) from the Trellix Download Server and save it in the Linux based Manager server when using **`install the setup present on local machine`** upgrade in 11.1.7.2 or other higher versions of Linux based Manager.

   NOTE

   Make a note of the location where the upgrade file is saved in the Manager server.

3. You must download the Manager upgrade file (setup.bin) from the Trellix Download Server and save it in the Linux machine, when using **`scp setup from remote machine and install`** upgrade in 11.1.7.2 or other higher versions of Linux based Manager versions.

> **NOTE**
>
> Make a note of the location where the upgrade file is saved in the Linux machine.

Steps:

- **If you are upgrading from Manager versions 11.1.7.2 or higher:**

  a. Log on to the restricted shell of Manager Appliance using default username and password.

  b. Stop the Watchdog service by executing **`watchdog stop`** command.

  c. Stop the Manager service by executing **`manager stop`** command.

  d. Execute the following command to upgrade the Manager:

  ```
  upgrade
  ```

  e. 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.

  f. If you select 1, continue with the following steps:

    1. 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**.

    2. 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**.

3. 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**.

4. 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`**.
5. After completing the upgrade procedure, check the Manager version using **`show managerVersion`** command to ensure successful upgrade.
6. Reboot the Linux based Manager by executing **`reboot`** command.

g. If you select 2, do the following:

1. 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**.

2. 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`**.
3. After completing the upgrade procedure, check the Manager version using **`show managerVersion`** command to ensure successful upgrade.
4. Reboot the Linux based Manager by executing **`reboot`** command.

Install Linux Operating Server in the Manager Appliance

Prerequisites:

Check the following before you install Linux based Manager in the Manager Appliance:

- Store the Linux based Manager installation bootup files on a FAT32 formatted USB drive.
- Check for physical access to the Appliance.

Steps:

1. Boot up the Manager Appliance with Linux based Manager bootable image file. For steps to install Manager Appliance (Linux) using a bootable image, see Installing Manager Appliance (Linux) using an ISO image (page 36).
2. Once the Manager Appliance is up, ensure that the server is accessible over network.

Installing Manager Appliance (Linux) using a bootable image

Prerequisites:

Copy the Linux-based Manager bootup files to a **USB drive** from a local folder or a shared location.

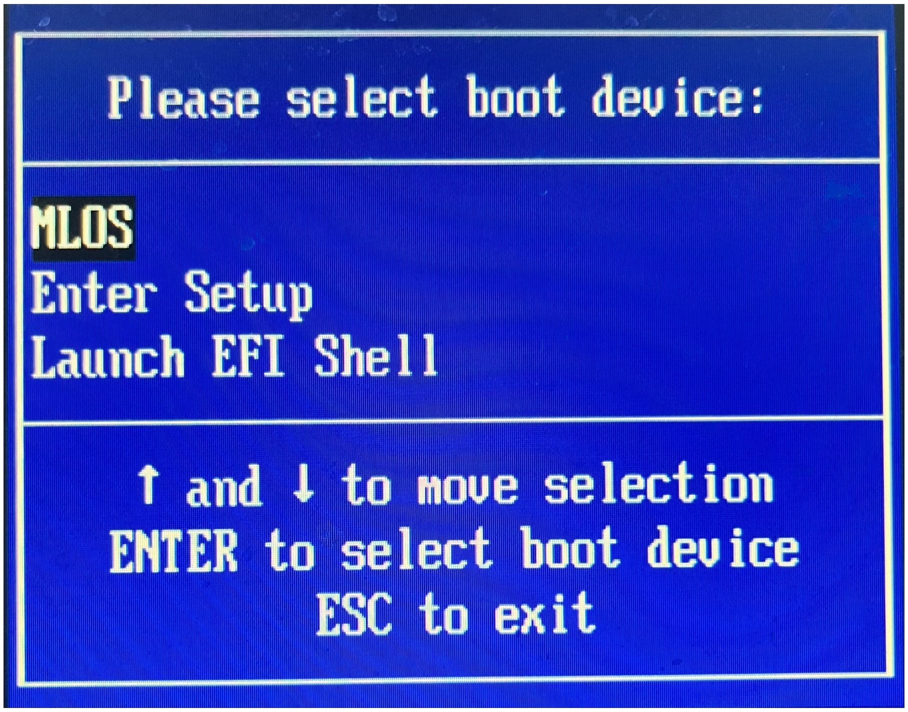
NOTE

For a bootable image of Linux-based Central Manager/Manager, Trellix recommends you to contact technical support at https://support.trellix.com.

Complete the steps below to install Manager Appliance (Linux) using a bootable image:

Steps:

1. Log in on to the Manager Appliance (Linux) using a console client.
2. Insert the **USB drive** in to the appliance.
3. Execute `reboot` command in the Manager Appliance console.
4. While the appliance is rebooting, press the **F6** key on the keyboard. The **Boot Manager** appears.
5. Select the **USB drive** name that you have inserted to the appliance.



```
Please select boot device:

MLOS
Enter Setup
Launch EFI Shell

↑ and ↓ to move selection
ENTER to select boot device
ESC to exit
```

NOTE

For the installation in the figure above, the name of the **USB drive** is SanDisk.

6. Press **Enter**. Boot up process starts.

NOTE

- You do not have to provide any inputs while the appliance is booting up.
- The Manager installation and boot up process will take around 45-60 minutes.

7. Once the Linux-based Manager is loaded and files copied, the message appears to **Remove the USB media**.
8. Remove the USB drive.

   The appliance reboots once the USB drive has been removed. On reboot, hardening scripts are executed and the Manager is installed.
9. You can configure the Manager with IP address, gateway address, netmask address, and DNS server address. For more information on Configuring the Manager Appliance, see Configuring the Manager Appliance (page 25).

Restore database to the Linux-based Manager Appliance

Prerequisites:

1. Make sure you have the backup file stored in the Linux machine where the Manager is installed.
2. If you have the backup files stored in a remote machine, use **`scpFromRemote`** command in Manager shell to copy the backup files to the Linux machine where the Manager is installed.

   Fore more information about **`scpFromRemote`** command, see the [SCP from remote] topic in the [CLI commands] section of the [Trellix Intrusion Prevention System Product Guide].

Steps:

1. Log in to the Manager shell using a console client with the credentials below:
   - Username: **`admin`**
   - Password: **`MLOSnsmApp`**

   NOTE

   The default password for Central Manager is **`MLOSnscmApp`**.

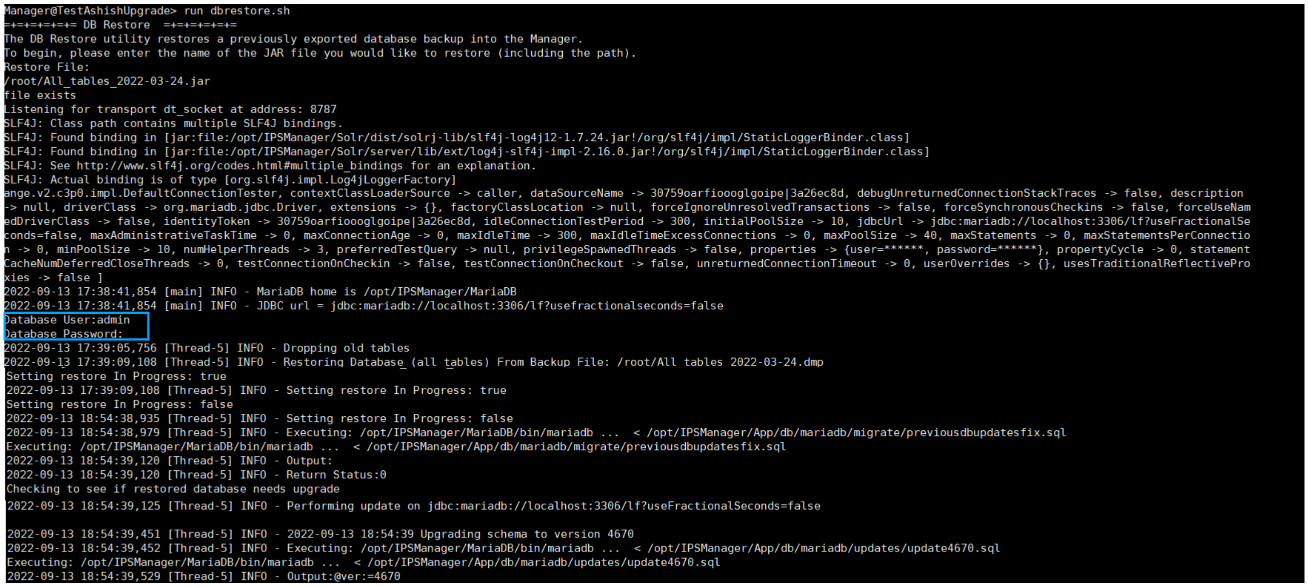
   NOTE

   SSH connection to the Linux-based Manager Appliance is not supported by Putty application. Trellix recommends you to use Tera Term application for remote access to the Manager Appliance using SSH.
2. Stop the Manager service using **`manager stop`** command in Manager shell.
3. Execute **`run dbrestore.sh`** command in the Manager shell.
4. Specify the backup file name at the **`Restore file`** prompt. For example, **`Restore file: /opt/scpfiles/dbbackup.jar`**.

NOTE

The default location of the database backup files copied to the Linux-based Manager using **`scpFromRemote`** command is **`/opt/scpfiles/`**.

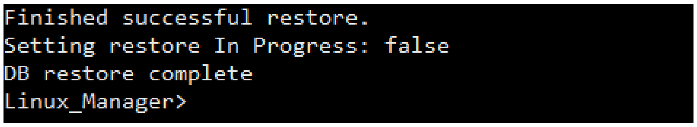
5. Specify the database user and password at the prompt.



```
Manager@TestAshishUpgrade> run dbrestore.sh
=+=+=+=+=+= DB Restore  =+=+=+=+=+=
The DB Restore utility restores a previously exported database backup into the Manager.
To begin, please enter the name of the JAR file you would like to restore (including the path).
Restore File:
/root/All_tables_2022-03-24.jar
file exists
Listening for transport dt_socket at address: 8787
SLF4J: Class path contains multiple SLF4J bindings.
SLF4J: Found binding in [jar:file:/opt/IPSManager/Solr/dist/solrj-lib/slf4j-log4j12-1.7.24.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: Found binding in [jar:file:/opt/IPSManager/Solr/server/lib/ext/log4j-slf4j-impl-2.16.0.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: See http://www.slf4j.org/codes.html#multiple_bindings for an explanation.
SLF4J: Actual binding is of type [org.slf4j.impl.Log4jLoggerFactory]
ange.v2.c3p0.impl.DefaultConnectionTester, contextClassLoaderSource -> caller, dataSourceName -> 30759oarfioooglgoipe|3a26ec8d, debugUnreturnedConnectionStackTraces -> false, description
-> null, driverClass -> org.mariadb.jdbc.Driver, extensions -> {}, factoryClassLocation -> null, forceIgnoreUnresolvedTransactions -> false, forceSynchronousCheckins -> false, forceUseNam
edDriverClass -> false, identityToken -> 30759oarfioooglgoipe|3a26ec8d, idleConnectionTestPeriod -> 300, initialPoolSize -> 10, jdbcUrl -> jdbc:mariadb://localhost:3306/lf?useFractionalSe
conds=false, maxAdministrativeTaskTime -> 0, maxConnectionAge -> 0, maxIdleTime -> 300, maxIdleTimeExcessConnections -> 0, maxPoolSize -> 40, maxStatements -> 0, maxStatementsPerConnectio
n -> 0, minPoolSize -> 10, numHelperThreads -> 3, preferredTestQuery -> null, privilegeSpawnedThreads -> false, properties -> {user=******, password=******}, propertyCycle -> 0, statement
CacheNumDeferredCloseThreads -> 0, testConnectionOnCheckin -> false, testConnectionOnCheckout -> false, unreturnedConnectionTimeout -> 0, userOverrides -> {}, usesTraditionalReflectivePro
xies -> false ]
2022-09-13 17:38:41,854 [main] INFO - MariaDB home is /opt/IPSManager/MariaDB
2022-09-13 17:38:41,854 [main] INFO - JDBC url = jdbc:mariadb://localhost:3306/lf?usefractionalseconds=false
Database User:admin
Database Password:
2022-09-13 17:39:05,756 [Thread-5] INFO - Dropping old tables
2022-09-13 17:39:09,108 [Thread-5] INFO - Restoring Database (all tables) From Backup File: /root/All tables 2022-03-24.dmp
Setting restore In Progress: true
2022-09-13 17:39:09,108 [Thread-5] INFO - Setting restore In Progress: true
Setting restore In Progress: false
2022-09-13 18:54:38,935 [Thread-5] INFO - Setting restore In Progress: false
2022-09-13 18:54:38,979 [Thread-5] INFO - Executing: /opt/IPSManager/MariaDB/bin/mariadb ...  < /opt/IPSManager/App/db/mariadb/migrate/previousdbupdatesfix.sql
Executing: /opt/IPSManager/MariaDB/bin/mariadb ...  < /opt/IPSManager/App/db/mariadb/migrate/previousdbupdatesfix.sql
2022-09-13 18:54:39,120 [Thread-5] INFO - Output:
2022-09-13 18:54:39,120 [Thread-5] INFO - Return Status:0
Checking to see if restored database needs upgrade
2022-09-13 18:54:39,125 [Thread-5] INFO - Performing update on jdbc:mariadb://localhost:3306/lf?useFractionalSeconds=false

2022-09-13 18:54:39,451 [Thread-5] INFO - 2022-09-13 18:54:39 Upgrading schema to version 4670
2022-09-13 18:54:39,452 [Thread-5] INFO - Executing: /opt/IPSManager/MariaDB/bin/mariadb ...  < /opt/IPSManager/App/db/mariadb/updates/update4670.sql
Executing: /opt/IPSManager/MariaDB/bin/mariadb ...  < /opt/IPSManager/App/db/mariadb/updates/update4670.sql
2022-09-13 18:54:39,529 [Thread-5] INFO - Output:@ver:=4670
```

The database restoration process starts. A success message is displayed at the completion of the process.



```
Finished successful restore.
Setting restore In Progress: false
DB restore complete
Linux_Manager>
```

Migrate alerts from MariaDB to Apache Solr in the Manager Appliance

The following section details the steps for migrating alerts from the MariaDB to the Apache Solr database in the Linux based Manager Appliance.

1. Log in to the Manager shell.
2. Stop the Manager service using the **`manager stop`** command.
3. Execute the following command block:

```
run solrImport.sh offline start days=<number of days>
```

When you run the Solr script, older alerts and other events for the required number of days are imported into Solr. You must specify the required number of days when you run the script for Apache Solr. For example, solrImport offline start days=25 imports 25 days of data.

4. Wait for the batch file to complete and then start the Manager service using the **`manager start`** command.

Maintaining Linux based Manager using Manager shell Utilities

InfoCollector utility

The InfoCollector utility collects and bundles essential Trellix IPS information for export or diagnosis.

To execute the InfoCollector script in the Manager shell, do the following:

1. Log in to the Manager shell using SSH.
2. Execute **`run InfoCollector.sh`** command to collect info logs.

   For collecting info logs by masking the sensitive information, execute **`run InfoCollector.sh -anon`** command.
3. (For InfoCollector in anonymous mode only) Select **`Update configuration`** in the operation menu and click **Enter**.
4. (For InfoCollector in anonymous mode only) Type **y** and click **Enter** when the following question is prompted:

   ```
   Do you want to procced with info collector bundle creation? [y/n]
   ```
5. Specify the log collection start date in the format [MM/DD/YYYY] and press **Enter**. Alternatively, just press **Enter** to choose the default start date (date preceding the current date).
6. Specify the log collection end date in the format [MM/DD/YYYY] and press **Enter**. Alternatively, just press **Enter** to choose the default end date (date preceding the current date).

   Select the type of log files to be collected. By default, InfoCollector collects Manager and Manager Configuration files only; however, you can control which items are collected as shown below:

   1. For default log file, specify **y** at Collect Default Items only prompt. The log bundle will be created with the filename in the format **`InfoLogs<Date><time>.zip`** along with success message.

      NOTE

      By default, InfoCollector collects Manager logs and Manager configuration files only. However, you can control which items are collected.

   2. For manually selecting custom sets of logs, specify **n** at the Collect Default Items only prompt. Now select the log files to be included in the bundle by specify **y** or **n** one by one for each type of log.

      The available log types are as follows:

      - Manager Logs
      - Configuration Backups
      - Audit Log Backups
      - Manager Configuration Files
      - Compiled 'Sigfiles' (Trellix Intrusion Prevention System Sensor Deployment Binaries)
      - System Faults

- Trellix Intrusion Prevention System Sensor Logs

> **NOTE**
>
> You can collect the Configuration Backups only when the InfoCollector utility is run in the normal mode.

A success message is displayed after the creation of InfoCollector bundle is completed.

> **NOTE**
>
> The InfoCollector bundle will be available in the following locations in the Manager:
>
> - **`/opt/IPSManager/App/diag/InfoCollector/InfoCollectorData/`**
> - **`/opt/scpfiles/`**

Database backup

The database backup script is used for taking a database back-up of the Linux based Manager.

Prerequisites:

1. Make sure you have a Linux machine in the network where the Linux based Manager is installed.

Perform database backup from the Linux based Manager/Central Manager as shown below:

Steps:

1. Log in to the Manager shell using SSH.
2. Stop the Manager service by executing **`manager stop`** command.
3. Execute **`run dbBackup.sh`** command in the Manager shell.
4. Enter the Manager Shell password when prompted.
5. Select the backup types to be included in the back up bundle.

   The backup types available for backup are as follows:

   1. ALL TABLES
   2. CONFIG TABLES
   3. AUDIT TABLES
   4. EVENT TABLES
   5. TREND TABLES
6. A success message is displayed after the creation of backup bundle is completed.

   The backup tables will be saved at **`opt/IPSManager/App/Backups/`**.
7. Execute **`moveManualBackups`** command to move the backup files from **`opt/IPSManager/App/Backups/`** to **`/opt/scpfiles`** folder.
8. Execute **`show files`** command to check the availability of backup files.

Database restore

The Database Restore script is used for restoring the backed-up database to the Manager running on Linux operating system.

Prerequisites:

1. Make sure you have the backup file stored in the Linux machine where the Manager is installed.
2. If you have the backup files stored in a remote machine, use **`scpFromRemote`** command in Manager shell to copy the backup files to the Linux machine where the Manager is installed.

   Fore more information about **`scpFromRemote`** command, see the [CLI commands] section in [Trellix Intrusion Prevention System Product Guide].

Perform database restore to the Linux-based Manager/Central Manager as shown below:

Steps:

1. Log in to the Manager shell using a console client with the credentials below:
   - Username: **`admin`**
   - Password: **`MLOSnsmApp`**

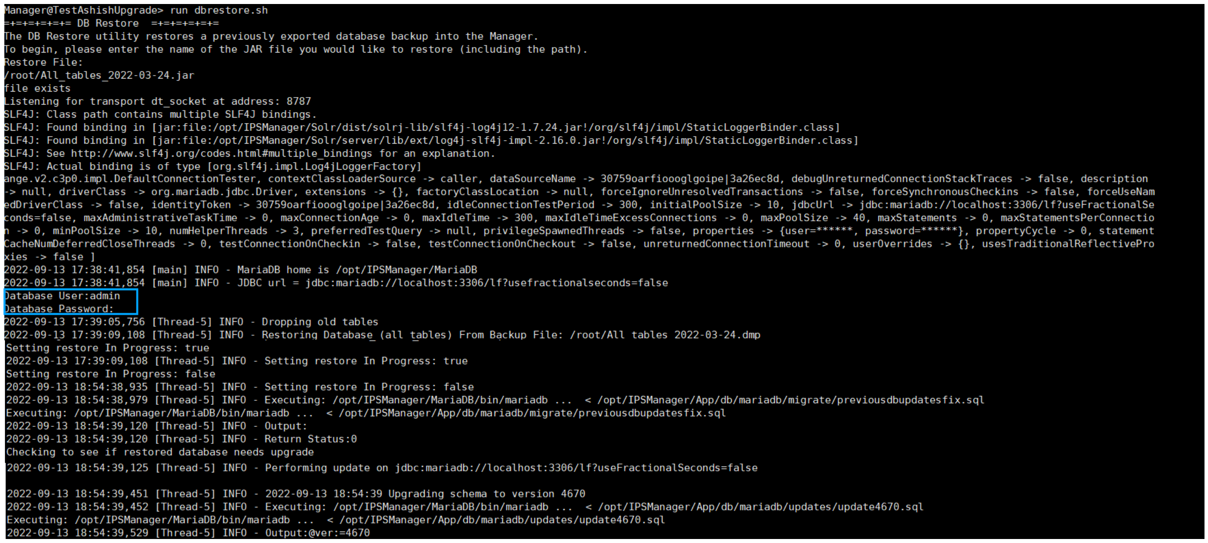
   > **NOTE**
   >
   > The default password for Central Manager is **`MLOSnscmApp`**.

   > **NOTE**
   >
   > SSH connection to the Linux-based Manager Appliance is not supported by Putty application. Trellix recommends you to use Tera Term application for remote access to the Manager Appliance using SSH.

2. Stop the Manager service using **`manager stop`** command in Manager shell.
3. Execute **`run dbrestore.sh`** command in the Manager shell.
4. Specify the backup file name at the **`Restore file`** prompt. Example: **`Restore file: /opt/scpfiles/dbback-up.jar`**.

   > **NOTE**
   >
   > The default location of the database backup files copied to the Linux-based Manager using **`scpFromRemote`** command is **`/opt/scpfiles/`**.

5. Specify the database user and password at the prompt.



```
Manager@TestAshishUpgrade> run dbrestore.sh
=+=+=+=+=+= DB Restore  =+=+=+=+=+=
The DB Restore utility restores a previously exported database backup into the Manager.
To begin, please enter the name of the JAR file you would like to restore (including the path).
Restore File:
/root/All_tables_2022-03-24.jar
file exists
Listening for transport dt_socket at address: 8787
SLF4J: Class path contains multiple SLF4J bindings.
SLF4J: Found binding in [jar:file:/opt/IPSManager/Solr/dist/solrj-lib/slf4j-log4j12-1.7.24.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: Found binding in [jar:file:/opt/IPSManager/Solr/server/lib/ext/log4j-slf4j-impl-2.16.0.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: See http://www.slf4j.org/codes.html#multiple_bindings for an explanation.
SLF4J: Actual binding is of type [org.slf4j.impl.Log4jLoggerFactory]
ange.v2.c3p0.impl.DefaultConnectionTester, contextClassLoaderSource -> caller, dataSourceName -> 30759oarfioooglgoipe|3a26ec8d, debugUnreturnedConnectionStackTraces -> false, description
-> null, driverClass -> org.mariadb.jdbc.Driver, extensions -> {}, factoryClassLocation -> null, forceIgnoreUnresolvedTransactions -> false, forceSynchronousCheckins -> false, forceUseNam
edDriverClass -> false, identityToken -> 30759oarfioooglgoipe|3a26ec8d, idleConnectionTestPeriod -> 300, initialPoolSize -> 10, jdbcUrl -> jdbc:mariadb://localhost:3306/lf?useFractionalSe
conds=false, maxAdministrativeTaskTime -> 0, maxConnectionAge -> 0, maxIdleTime -> 300, maxIdleTimeExcessConnections -> 0, maxPoolSize -> 40, maxStatements -> 0, maxStatementsPerConnectio
n -> 0, minPoolSize -> 10, numHelperThreads -> 3, preferredTestQuery -> null, privilegeSpawnedThreads -> false, properties -> {user=******, password=******}, propertyCycle -> 0, statement
CacheNumDeferredCloseThreads -> 0, testConnectionOnCheckin -> false, testConnectionOnCheckout -> false, unreturnedConnectionTimeout -> 0, userOverrides -> {}, usesTraditionalReflectivePro
xies -> false ]
2022-09-13 17:38:41,854 [main] INFO - MariaDB home is /opt/IPSManager/MariaDB
2022-09-13 17:38:41,854 [main] INFO - JDBC url = jdbc:mariadb://localhost:3306/lf?usefractionalseconds=false
Database User:admin
Database Password:
2022-09-13 17:39:05,756 [Thread-5] INFO - Dropping old tables
2022-09-13 17:39:09,108 [Thread-5] INFO - Restoring Database (all tables) From Backup File: /root/All tables 2022-03-24.dmp
Setting restore In Progress: true
2022-09-13 17:39:09,108 [Thread-5] INFO - Setting restore In Progress: true
Setting restore In Progress: false
2022-09-13 18:54:38,935 [Thread-5] INFO - Setting restore In Progress: false
2022-09-13 18:54:38,979 [Thread-5] INFO - Executing: /opt/IPSManager/MariaDB/bin/mariadb ...  < /opt/IPSManager/App/db/mariadb/migrate/previousdbupdatesfix.sql
Executing: /opt/IPSManager/MariaDB/bin/mariadb ...  < /opt/IPSManager/App/db/mariadb/migrate/previousdbupdatesfix.sql
2022-09-13 18:54:39,120 [Thread-5] INFO - Output:
2022-09-13 18:54:39,120 [Thread-5] INFO - Return Status:0
Checking to see if restored database needs upgrade
2022-09-13 18:54:39,125 [Thread-5] INFO - Performing update on jdbc:mariadb://localhost:3306/lf?useFractionalSeconds=false

2022-09-13 18:54:39,451 [Thread-5] INFO - 2022-09-13 18:54:39 Upgrading schema to version 4670
2022-09-13 18:54:39,452 [Thread-5] INFO - Executing: /opt/IPSManager/MariaDB/bin/mariadb ...  < /opt/IPSManager/App/db/mariadb/updates/update4670.sql
Executing: /opt/IPSManager/MariaDB/bin/mariadb ...  < /opt/IPSManager/App/db/mariadb/updates/update4670.sql
2022-09-13 18:54:39,529 [Thread-5] INFO - Output:@ver:=4670
```

With this, the Database restoration process starts and a success message is displayed at the completion of the process.

Change Database Password

The following section details the procedure to change the Manager database password in the Manager shell.

Change the Admin user password for the Manager database

The following section details the procedure to change the Manager database admin user password in the Manager shell.

1. Log in to the Manager shell using SSH.
2. Stop the Manager service using **`manager stop`** command
3. Execute **`run passwordchange.sh`** command in the Manager shell.
4. Specify the **MariaDB Root Password** at the prompt. The default password is **`root123`**.
5. Specify the **Database's Current 'admin' Password** (Manager database admin user) password at the prompt. By default, the password for the application is **`admin123`**.
6. Specify the **New Database admin Password** and **Confirm New Password** for the Manager database.

On completion, a success message for the password change is displayed.

Change the Root user password for the Manager database

The following section details the procedure to change the Manager database root user password in the Manager shell.

1. Log in to the Manager shell using SSH.
2. Execute **`run changeDbRootPass.sh`** command in the Manager shell.

3. Specify the **Current db password** (Manager database root user) at the prompt. The default password is **`root123`**.
4. Specify the **New db password** and **Confirm the new db password** for the Manager database root user.

On completion, a success message for the password change is displayed.

Opt partition extension in Linux based Manager

The Manager application uses opt partition in the disk space to store all information. Perform the following steps to extend the opt partition to avoid the Manager application running out of disk space in a Linux based Manager.

Prerequisite:

Take an ALL TABLES database backup of the Linux based Manager and store it in a remote machine.

> **NOTE**
>
> You can extend the opt partition only in the Linux based Manager virtual 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 (that is, 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 opt partition:

```
vgextend fs /dev/<new_sda>
```

Parameter	Description
new_sda	Specify the name of the newly created sda.

21. Execute the below command block:

```
lvextend -L+<memory_extended>G /dev/mapper/fs-opt
```

Parameter	Description
`memory_extended`	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 **`memory_extented`** value should be entered as 50.

22. Execute **`df -h`** and make a note of **`/dev/mapper/fs-opt`** filesystem size.
23. Execute the command block below to resize the **`/dev/mapper/fs-opt`** filesystem size.

    ```
    resize2fs /dev/mapper/fs-opt
    ```

24. Execute **`df -h`** and verify that the **`/dev/mapper/fs-opt`** filesystem size is extended.

How to configure rsyslog server in Linux-based Manager

If you need to establish communication with a different port, you must define the required port using **`semanage`**. You can define the required port for rsyslog server connection in Linux-based Manager for the following three protocols:

- UDP
- TCP
- TCP over SSL

To establish a rsyslog connection using a required port, execute the following command after enabling the port in the firewall:

```
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.

You can refer the below sections to establish rsyslog communication in Linux-based Manager.

How to establish UDP connection between the rsyslog server and the Manager

To establish UDP connection between the rsyslog server and the Manager client machine, do the following:

Prerequisites:

- Make sure the rsyslog service is running in the rsyslog server.
- Make sure the rsyslog service is running in the Manager client machine.
- Make sure the clocks in the rsyslog server and the client machine are synchronized.

Steps:

1. Perform the following in the rsyslog server:
   a. Open command prompt.
   b. Make sure the port 514 in the rsyslog server is open using the **`netstat`** command.
   c. (Optional) Execute the following command block to open the port 514 in the rsyslog server:

      ```
      # firewall-cmd --permanent --add-port=514/udp
      # firewall-cmd –reload
      ```

   d. (Optional) Repeat step b.
   e. Execute the command **`vi /etc/rsyslog.conf`** to open the **`rsyslog.conf`** file.

   f. Add the following entries to the **rsyslog.conf** file to configure UDP protocol:

      ```
      $ModLoad imudp
      $UDPServerRun 514
      ```

   g. Restart rsyslog service using the **systemctl restart rsyslog** command.

2. Perform the following in the Linux based Manager:

   a. Log in to the Manager shell.

   b. Make sure the port 514 in the Manager is open using the **netstat** command.

   c. (Optional) Execute the following command block to open the port 514 in the Manager:

      ```
      # firewall_cmd --permanent --add-port=514/udp
      # firewall_cmd –reload
      ```

   d. (Optional) Repeat step b.

   e. Execute the command **edit rsyslog.conf** to open the **rsyslog.conf** file.

   f. Add the following entry to the **rsyslog.conf** file to configure UDP protocol:

      ```
      *.* @<rsyslog Server IP Address or Domain Name>:514
      ```

   g. Restart the syslog service using the **syslog restart** command.

3. To verify the UDP connection, execute **logger "<message to be sent to the rsyslog server>"** command in the Manager shell and verify if the same message is available in **/var/log/messages** file in the rsyslog server.

How to establish TCP connection between the rsyslog server and the Manager

To establish TCP connection between the rsyslog server and the Manager client machine, do the following:

Prerequisites:

- Make sure the rsyslog service is running in the rsyslog server.
- Make sure the rsyslog service is running in the Manager client machine.
- Make sure the clocks in the rsyslog server and the client machine are synchronized.

Steps:

1. Perform the following in the rsyslog server:

   a. Open command prompt.

   b. Make sure the port 514 in the rsyslog server is open using the **netstat** command.

   c. (Optional) Execute the following command block to open the port 514 in the rsyslog server:

      ```
      # firewall-cmd --permanent --add-port=514/tcp
      # firewall-cmd –reload
      ```

   d. (Optional) Repeat step b.

   e. Execute the command **vi /etc/rsyslog.conf** to open the **rsyslog.conf** file.

   f. Add the following entries to the **rsyslog.conf** file to configure TCP protocol:

```
$ModLoad imtcp
$InputTCPServerRun 514
```

   g. Restart rsyslog service using the **`systemctl restart rsyslog`** command.

2. Perform the following in the Linux based Manager:

   a. Log in to the Manager shell.

   b. Make sure the port 514 in the Manager is open using the **`netstat`** command.

   c. (Optional) Execute the following command block to open the port 514 in the Manager:

   ```
   # firewall_cmd --permanent --add-port=514/tcp
   # firewall_cmd –reload
   ```

   d. (Optional) Repeat step b.

   e. Execute the command **`edit rsyslog.conf`** to open the **`rsyslog.conf`** file.

   f. Add the following entry to the **`rsyslog.conf`** file to configure TCP protocol:

   ```
   *.* @@<rsyslog Server IP Address or Domain Name>:514
   ```

   g. Restart the syslog service using the **`syslog restart`** command.

3. To verify the TCP connection, execute **`logger "<message to be sent to the rsyslog server>"`** command in the Manager shell and verify if the same message is available in **`/var/log/messages`** file in the rsyslog server.

How to establish TCP over SSL connection between the rsyslog server and the Manager

To establish TCP over SSL connection between the rsyslog server and the Manager client machine, do the following:

Prerequisites:

- Make sure the rsyslog service is running in the rsyslog server.
- Make sure the rsyslog service is running in the Manager client machine.
- Make sure the clocks in the rsyslog server and the client machine are synchronized.

Steps:

1. Log in to the Manager shell.
2. Create a self-signed CA certificate in the Linux based Manager to sign the certificate for establishing trust between the Manager and the rsyslog server.

   a. Execute the following command block to create a private key for the self-signed CA certificate:

   ```
   certtool --generate-privkey --outfile ca-key.pem
   ```

   b. Execute the following command block to create the self-signed CA certificate:

   ```
   certtool --generate-self-signed --load-privkey ca-key.pem --outfile ca.pem
   ```

   c. Provide the details for the certificate as needed when the following configuration options are displayed:

Options	Action
Common name	Enter a name for the certificate and press **Enter**.

Options	Action
UID	Enter a unique identification number for the certificate and press **Enter**.
Organizational unit name	Enter the organization unit name for the certificate and press **Enter**.
Organization name	Enter the organization name for the certificate and press **Enter**.
Locality name	Enter the locality of the Linux based Manager and press **Enter**.
State or province name:	Enter the State or province name of the Linux based Manager and press **Enter**.
Country name (2 chars)	Enter the country name of the Linux based Manager and press **Enter**.
Enter the subject's domain component (DC)	Enter the domain component of the Linux based Manager and press **Enter**.
Email	Enter an email ID for the certificate and press **Enter**.
Enter the certificate's serial number in decimal	Enter a serial number for the certificate and press **Enter**.
Activation/Expiration time. The certificate will expire in (days)	Enter the validity of the certificate in days and press **Enter**.
Does the certificate belong to an authority? (y/N)	Type **y** and press **Enter**.
Path length constraint (decimal, -1 for no constraint)	Type **`-1`** and press **Enter**.
Is this a TLS web client certificate? (y/N)	Type **n** and press **Enter**.
Will the certificate be used for IPsec IKE operations? (y/N)	Type **n** and press **Enter**.
Is this a TLS web server certificate? (y/N)	Type **n** and press **Enter**.
Enter a dnsName of the subject of the certificate	Enter the DNS name of the Linux based Manager and press **Enter**.
Enter a URI of the subject of the certificate	Enter the URI of the Linux based Manager and press **Enter**.
Enter the IP address of the subject of the certificate	Enter the IP address of the Linux based Manager and press **Enter**.

Options	Action
Enter the email of the subject of the certificate	Enter an email address for the certificate and press **Enter**.
Will the certificate be used to sign OCSP requests?	Type **n** and press **Enter**.
Will the certificate be used to sign code?	Type **n** and press **Enter**.
Will the certificate be used for time stamping?	Type **n** and press **Enter**.
Will the certificate be used to sign other certificates?	Type **y** and press **Enter**.
Will the certificate be used to sign CRLs?	Type **y** and press **Enter**.

d. Type **yes** and press **Enter** when the following question is prompted:

```
Is the above information ok? (y/N):
```

3. Create a request certificate for the self-signed CA signed certificate for establishing trust between the Linux based Manager and the rsyslog server.

a. Execute the following command block to create a private key for the request certificate:

```
certtool --generate-privkey --outfile server-key.pem --bits 2048
```

b. Execute the following command block to create the request certificate:

```
certtool --generate-request --load-privkey server-key.pem --outfile server-request.pem
```

c. Provide the details for the certificate as needed when the following configuration options are displayed:

Options	Action
Common name	Enter a name for the certificate and press **Enter**.
Organizational unit name	Enter the organization unit name for the certificate and press **Enter**.
Organization name	Enter the organization name for the certificate and press **Enter**.
Locality name	Enter the locality of the rsyslog server and press **Enter**.
State or province name:	Enter the province of the rsyslog server locality and press **Enter**.
Country name (2 chars)	Enter the country name of the rsyslog server and press **Enter**.
Enter the subject's domain component (DC)	Enter the component of the rsyslog server using the certificate.
UID	Enter a unique identification number for the certificate and press **Enter**.

Options	Action
Enter a dnsName of the subject of the certificate	Enter the DNS name of the rsyslog server.
Enter a URI of the subject of the certificate	Enter the URI of the rsyslog server.
Enter the IP address of the subject of the certificate	Enter the IP address of the rsyslog server.
Enter the email of the subject of the certificate	Enter the email ID for the rsyslog server and press **Enter**.
Enter a challenge password:	Enter a password for the certificate and press **Enter**.
Does the certificate belong to an authority?	Type **y** and press **Enter**.
Will the certificate be used for signing (DHE and RSA-EXPORT cipher suites)?	Type **n** and press **Enter**.
Will the certificate be used for encryption (RSA ciphersuites)?	Type **n** and press **Enter**.
Will the certificate be used to sign code? (y/N)	Type **n** and press **Enter**.
Will the certificate be used for time stamping?	Type **n** and press **Enter**.
Will the certificate be used for IPsec IKE operations?	Type **n** and press **Enter**.
Will the certificate be used to sign OCSP requests?	Type **n** and press **Enter**.
Is this a TLS web client certificate?	Type **n** and press **Enter**.
Is this a TLS web server certificate?	Type **n** and press **Enter**.

d. Type **yes** and press **Enter** when the following question is prompted:

```
Is the above information ok? (y/N):
```

4. Create a self-signed CA signed certificate for establishing trust between the Manager and the rsyslog server.

a. Execute the following command block to create the self-signed CA signed certificate:

```
certtool --generate-certificate --load-request server-request.pem --outfile server-
cert.pem --load-ca-certificate ca.pem --load-ca-privkey ca-key.pem
```

b. Provide the details for the certificate as needed when the following configuration options are displayed:

Options	Action
Enter the certificate's serial number in decimal	Enter a serial number for the certificate and press **Enter**.
Activation/Expiration time. The certificate will expire in (days)	Enter the validity of the certificate in days and press **Enter**.
Do you want to honour the extensions from the request?	Press **Enter** to confirm.
Does the certificate belong to an authority? (y/N)	Type **y** and press **Enter**.
Is this a TLS web client certificate? (y/N)	Type **y** and press **Enter**.
Will the certificate be used for IPsec IKE operations? (y/N)	Press **Enter**.
Is this a TLS web server certificate? (y/N)	Type **y** and press **Enter**.
Enter a dnsName of the subject of the certificate	Enter the DNS name of the rsyslog server and press **Enter**.
Enter a URI of the subject of the certificate	Enter the URI of the rsyslog server and press **Enter**.
Enter the IP address of the subject of the certificate	Enter the IP address of the rsyslog server and press **Enter**.
Will the certificate be used for signing (DHE and RSA-EXPORT cipher suites)?	Type **n** and press **Enter**.
Will the certificate be used for encryption (RSA ciphersuites)?	Type **n** and press **Enter**.

Options	Action
Will the certificate be used to sign OCSP requests?	Type **n** and press **Enter**.
Will the certificate be used to sign code?	Type **n** and press **Enter**.
Will the certificate be used for time stamping?	Type **n** and press **Enter**.

c. Type **yes** and press **Enter** when the following question is prompted:

```
Is the above information ok? (y/N):
```

5. Make sure the certificate files are available in **/opt/scpfiles** location using the **show files** command.
6. Using the **scpToremote** command copy the ca.pem, server-cert.pem, and server-key.pem to the rsyslog server.
7. Move the certificates to **/etc/syslogcerts** location using the **copyCertsToSyslogDir** command.
8. Perform the following in the rsyslog server:

   a. Open command prompt.

   b. Make sure the port 10514 in the rsyslog server is open using the **netstat** command.

   c. (Optional) Execute the following command block to open the port 10514 in the rsyslog server:

```
# firewall-cmd --permanent --add-port=10514/tcp
# firewall-cmd –reload
```

   d. (Optional) Repeat step b.

   e. Execute the command **vi /etc/rsyslog.conf** to open the **rsyslog.conf** file.

   f. Add the following entries to the **rsyslog.conf** file to configure TCP protocol:

```
# make gtls driver the default
$DefaultNetstreamDriver gtls
# certificate files
$DefaultNetstreamDriverCAFile /etc/syslogcerts/ca.pem
$DefaultNetstreamDriverCertFile /etc/syslogcerts/server-cert.pem
$DefaultNetstreamDriverKeyFile /etc/syslogcerts/server-key.pem
$ModLoad imtcp  # TCP listener
$InputTCPServerStreamDriverMode 1  # run driver in TLS-only mode
$InputTCPServerStreamDriverAuthMode anon
$InputTCPServerRun 10514  # start up listener at port 10514
```

   g. Restart rsyslog service using the **systemctl restart rsyslog** command.

9. Perform the following in the Linux based Manager:

   a. Log in to the Manager shell.

   b. Make sure the port 10514 in the Manager is open using the **netstat** command.

c. (Optional) Execute the following command block to open the port 10514 in the Manager:

```
# firewall_cmd --permanent --add-port=10514/tcp
# firewall_cmd –reload
```

d. (Optional) Repeat step b.

e. Execute the command **edit rsyslog.conf** to open the **rsyslog.conf** file.

f. Add the following entry to the **rsyslog.conf** file to configure TCP protocol:

```
# certificate files
$DefaultNetStreamDriverCAFile /etc/syslogcerts/ca.pem
# make gtls driver the default
$DefaultNetStreamDriver gtls
$ActionSendStreamDriverMode 1    # run driver in TLS-only mode
$ActionSendStreamDriverAuthMode anon
*.* @@<rsyslog Server IP Address / Domain Name>:10514
```

g. Restart the syslog service using the **syslog restart** command.

10. To verify the TCP over SSL connection, execute **logger "<message to be sent to the rsyslog server>"** command in the Manager shell and verify if the same message is available in **/var/log/messages** file in the rsyslog server.

Configuration of NTP with SHA1 authentication

To configure the Network time Protocol (NTP) with SHA1 authentication on the server machine (Remote), do the following:

1. Log in to the remote machine (Server).
2. Execute the command **ntp-keygen -M**

   This generates a **ntp.keys** file with a list of md5 and sha1 keys.
3. Execute the command **vi /etc/ntp.conf** to open the **ntp.conf** file.
4. Add **server <IP/domain name of the time server>** to the **ntp.conf** file.
5. Configure the **keys** attribute by replacing the default path **/etc/ntp/keys** with **/<navpath>/ntp.keys** or copy the content of the **ntp.keys** file to **/etc/ntp/keys**.
6. Configure the **trustedkey** attribute by adding the serial no. or Id of any one of the SHA1 key present in the **ntp.keys** file. For example, **trustedkey 13**.
7. Save and exit from the vi editor.
8. Execute the command **systemctl restart ntpd** as the configuration of **ntp.conf** file was changed.

To configure the Network time Protocol (NTP) with SHA1 authentication on the client machine (Manager), do the following:

1. Login to the Manager shell.
2. Execute the command **edit ntp.keys**.
3. Add the trusted key that was mentioned in the server machine from server **ntp.keys** file (In this example, Trustedkey value 13).
4. Save and exit from the vi editor.

5. Execute command **`edit ntp.conf`**.
6. Add **`server <IP of the server machine> key <trusted key id>`**. For example, **`server 10.2.1.1 key 13`**.
7. Configure the **`trustedkey`** attribute by adding the serial no. or Id of any one of the SHA1 key present in the **`ntp.keys`** file. For example, **`trustedkey 13`**.
8. Save and exit from the vi editor.
9. Execute the command **`systemctl restart ntpd`**.
10. Execute the command **`ntpstat`** after 15 minutes to check if the time is synchronized.

Procedure to update uvscan signature in an air-gapped network

To update the uvscan signature in an air-gapped network, do the following:

1. Download the latest dat file from https://download.nai.com/products/commonupdater/current/vscandat1000/dat/0000/.

   The file name downloaded will be in the format **`avvdat-<xxxx>.zip`**.
2. Log in to the Manager shell.
3. Copy the file on the Manager using SCP or SFTP.
4. Execute **`avvdat -i/<navpath of the scpfiles>/<xxx>.zip`** command to update the uv scan signature in an air-gapped network.

Procedure to update avvdat signatures

To update the avvdat signatures, do the following:

1. Log in to the Manager shell.
2. If you have proxy configured in your network, perform the following steps. If not, perform step 3.
   a. Execute the **`edit environment`** command.

   > **NOTE**
   >
   > This command will edit the file using vi-editor. Trellix recommends you to use **`vi_editor`** commands to perform operations on the files.

   b. Enter proxy details. For example, refer to the following format:
   - **`MY_PROXY_URL="<proxy server url or ip>:<proxy server port>"`**
   - **`HTTP_PROXY=$MY_PROXY_URL`**
   - **`HTTPS_PROXY=$MY_PROXY_URL`**
   - **`FTP_PROXY=$MY_PROXY_URL`**
   - **`http_proxy=$MY_PROXY_URL`**
   - **`https_proxy=$MY_PROXY_URL`**
   - **`ftp_proxy=$MY_PROXY_URL`**
   - **`export HTTP_PROXY HTTPS_PROXY FTP_PROXY http_proxy https_proxy ftp_proxy`**

   c. Reboot and restart the system.

3. Execute the command **`avvdat -a`**.

Procedure to exclude directories from system anti-virus scan

To exclude directories from system anti-virus scan, do the following:

1. Log in to the Manager shell.
2. Execute the **`edit avexclusionlist`** command.

> **NOTE**
>
> This command will edit the file using vi-editor. Trellix recommends you to use **`vi_editor`** commands to perform operations on the files.

3. Add the directory paths that you want to exclude (For example, **`/home/admin`**).
4. Save the changes and exit the vi-editor.

Backup and restoration of operating system, Linux based Manager configuration and log files

To perform backup of system config file, execute the command **`system config backup`** to take the backup.

Backup gets created under **`/opt/scpfiles`** by the name of **`sysConfBackup_xxxx_xx_xx_xx_xx_xx.tar`**.

To perform the restoration of system config file, do the following:

1. Upload the backup .tar file to the Manager shell through SFTP or remote SCP.
2. Execute the command **`system config restore`** to restore the backup file form the same machine or remote machine, and provide the file path and details. For more information refer to the [CLI commands] section in [Trellix Intrusion Prevention System Product Guide].
3. Once restored, the configuration can be checked by using the command **`edit <file name>`**.

   The backup logs can be checked by using the command **`show backup log all`** or **`show backup log <file_name>`**.

Remote Monitoring and Management for the Linux based Manager Appliance

To configure Remote Monitoring and Management (RMM) for the Linux based Manager Appliance, do the following:

1. Reboot the Linux based Manager Appliance using the **`reboot`** command.
2. Press F2 while the Linux based Manager Appliance is booting.

   The **BIOS Settings** page opens.
3. Navigate to **Server Management** and press **Enter**.
4. Go to **Plug & Play BMC Detection** and press **Enter**.
5. Select **Enabled** and press **Enter**.
6. Navigate to **Console Redirection** and **Enable SOL for Baseboard Management** for **Management** and **Management NIC** .
7. Navigate to BMC LAN Configuration → **Dedicated Management LAN Configuration** and configure the following:

Option	Action
IP Source	Select **Static** and press **Enter**.
IP Address	Enter the IP address for the BMC Web Console interface of the Linux based Manager Appliance and press **Enter**. **NOTE** Use **Mgmt** port on the rear end of the Linux based Manager Appliance for the Web Console interface network configurations.
Subnet Mask	Enter the subnet mask for the Web Console interface of the Linux based Manager Appliance and press **Enter**.
Gateway IP	Enter the Gateway IP address for the Web Console interface of the Linux based Manager Appliance and press **Enter**.
User Configuration for User 2	
Privileges	Select **Administrator** and press **Enter**.
User Status	Select **Enabled** and press **Enter**.
Username	Enter a username for accessing the Integrated BMC Web Console interface and press **Enter**.
User Password	Enter and confirm the password for accessing the Integrated BMC Web Console interface and press **Enter**.

8. Press F10 to save the changes and then press **Enter**.

Log on to the Integrated BMC Web Console interface:

1. Open a new web browser session.
2. In the address bar, type **`https://<IP Address assigned to the BMC Web Console interface>`**.
3. For User and Password, type your username and password as configured in the BIOS settings.

Troubleshooting

This section provides information on common issues that you may encounter as you configure and use the Manager Appliance.

The Manager Appliance is not receiving power

If the appliance is not receiving power, check for the following options.

- The Manager Appliance is connected properly to a working power outlet, using the supplied power cord. If the power outlet has a switch, make sure it is on.
- The Manager Appliance is correctly switched on.
- The power cord is plugged in to the back of the Manager Appliance.

If the Manager Appliance is still not receiving power, check the power outlet by plugging other equipment into it. If the power outlet is working, there is a problem with the Manager Appliance or its power cord.

The Manager Appliance will not start

If the system information lights on the front panel do not appear after the Manager Appliance has had reasonable time to boot, the problem may be an IP address conflict with another computer on your network.

To resolve this problem, configure the NICs to ensure they use only available IP addresses on your network. To do this, see Configuring Manager Appliance (page 23) section of this guide. Trellix recommends that you use static IP address(es) for the Manager Appliance.

The Manager Appliance is not communicating with the network

Look for these options if the appliance is not receiving network traffic.

Check the following:

- The Manager Appliance is turned on and its software is running, indicated by the lights on the front display panel.
- The Manager Appliance has a valid IP address and can ping the gateway (or can be pinged from another system).
- The network cables that you are using are undamaged and connected properly to the Manager Appliance ports and your existing network equipment. Make sure that the cables you use have the correct specifications.
- You have used the correct LAN ports when connecting the Manager Appliance to your existing network equipment.
- You used NIC 1 for configuring the system; if not, try connecting via NIC 1 and perform the configuration process again.

If the Manager Appliance is still not receiving network traffic, check the network cables and the network ports on your existing network equipment. If the cables and ports are working, there is a problem with the Manager Appliance. Contact your supplier.

Troubleshooting a hardware failure

If you suspect a hardware failure, contact Trellix Technical Support.

TIP

Trellix recommends you troubleshoot all hardware issues in conjunction with a Technical Support Technician.

Steps to disable or enable ports on firewall in MLOS

You can disable or enable firewall ports in MLOS to allow or block communication over these ports.

Procedure to disable or enable firewall ports varies depending on the NIC configuration and interface management on single or multiple firewall zones. Refer to the following scenarios for more information:

Scenario 1

The system is configured in single NIC or dual NIC configuration. Essentially the NIC interface(s) are in a single zone (by default in public zone). In this scenario, if a port needs to be blocked for one IP address in single NIC configuration or both IP addresses in dual NIC configuration, execute the following command:

`firewall_cmd --zone=public --permanent --remove-port=<port>/<protocol>`

Upon executing the above command, refresh the firewall configuration by issuing the command **`firewall_cmd --reload`**, followed by MLOS reboot.

Below given are the examples of blocking a single TCP port and a TCP port range:

- Command to block a single TCP port, for instance, port 3306: **`firewall_cmd --zone=public --permanent --remove-port=3306/tcp`**
- Command to block a TCP port range, for instance, ports 8501-8504: **`firewall_cmd --zone=public --permanent --remove-port=8501-8504/tcp`**
- Upon executing these command, refresh the firewall configuration by issuing the command **`firewall_cmd --reload`**, followed by MLOS reboot.

NOTE

Ports added in a range can only be removed as a range and not as individuals. If a single or multiple ports out of the range needs to be unblocked then the range needs to blocked/removed and then, the port(s) to be allowed needs to be added.

Scenario 2

There is only one zone present and managed by the firewall. In this scenario, we can add a rule to reject any request that comes to the system on a specific port for a specific IP address. The procedure is as follows:

Execute the command **`firewall_cmd --permanent --zone=public --add-rich-rule='rule family=ipv4 source address="<ip for which port needs to blocked>/<gateway>" port port="<port>/<port-range>" protocol="<tcp/udp>" reject'`**.

Upon executing the above command, refresh the firewall configuration by issuing the command **`firewall_cmd --reload`**, followed by MLOS reboot.

Upon reboot, execute the command **`firewall_cmd --list-all`** to view the updated configuration.

- For example, if the user wants to create a firewall rule to reject any traffic entering the IP subnet **`10.1.1.1/24`** on TCP port group **`8501-8504`** in **`public`** zone, execute the command **`firewall_cmd --permanent --zone=public --add-rich-rule='rule family=ipv4 source address="10.1.1.1/24" port port="8501-8504" protocol="tcp" reject'`**.
- Refresh the firewall configuration and reboot the system for the configuration update to happen.

Scenario 3

MLOS is set up with a dual NIC configuration and a user wants to manage interfaces separately in 2 different firewall zones. In this scenario, the procedure is as follows:

Execute the commands:

- **`firewall_cmd --permanent --new-zone=<zone name>`** to add a new firewall zone.
- **`firewall_cmd --get-zones`** to verify if the zone has been added.
- **`firewall_cmd --add-service=<service name><or><port>/<protocol><or><port-group>/<protocol> --zone=<zone name> --permanent`** to add a service (or) port (or) port group to the newly added zone.

- **`firewall_cmd --reload`** to refresh the firewall configuration, followed by MLOS reboot.
- **`firewall_cmd --list-all`** after reboot, to view the configuration.

For example, if user wants to create a new zone named **`work`** and block the TCP ports **`8501-8504`** on this zone, execute the following commands:

- **`firewall_cmd --permanent --new-zone=work`**
- **`firewall_cmd --zone=work --remove-port=8501-8504/tcp --permanent`**
- **`firewall_cmd --reload`** to refresh the firewall configuration, followed by MLOS reboot.

NOTE

Here, assumption is that the user wants to remove TCP ports 8501-8504. However, the same procedure can be followed for any port by excluding addition of that port(s) in the new zone and adding the rest of them.

Similarly, if user wants to allow **`https`** and **`ssh`** services and TCP ports **`9798`** and **`3306`** on the **`work`** zone, execute the following commands:

- **`firewall_cmd --add-service=https --zone=work --permanent`**
- **`firewall_cmd --add-service=ssh --zone=work --permanent`**
- **`firewall_cmd --zone=work --add-port=9798/tcp --permanent`**
- **`firewall_cmd --zone=work --add-port=3306/tcp --permanent`**
- **`firewall_cmd --reload`** to refresh the firewall configuration, followed by MLOS reboot.

If user wants to block traffic coming on interface **`eth0`** on **`work`** zone and allow traffic coming on interface **`eth0`** on **`public`** zone, execute the following commands:

- **`firewall_cmd --remove-interface=eth0 --zone=work`**
- **`firewall_cmd --add-interface=eth0 --zone=public`**
- **`firewall_cmd --reload`** to refresh the firewall configuration, followed by MLOS reboot.
- **`firewall_cmd --info-zone=work`** upon reboot to view the **`work`** zone configuration.
- **`firewall_cmd --info-zone=public`** to view the **`public`** zone configuration.

NOTE

At this point, check if the TCP ports 8501-8504 are accessible on defined private/public IP address. Ideally, they should not be accessible. If they are still accessible, execute the command **`firewall_cmd --permanent --zone=work --add-rich-rule='rule family=ipv4 port port=8501-8504 protocol=tcp reject'`**. This will add a rule to the firewall to reject any connection request(s) coming to these ports.

Upon executing the command, refresh the firewall configuration by issuing the command **`firewall_cmd --reload`**, followed by MLOS reboot. Then, execute the command **`firewall_cmd --info-zone=work`** to view the **`work`** zone configuration.

Procedure to check if the port is accessible for an IP address or not:

Execute the following commands from a remote machine which is on the same subnet as the private IP addresses will not be accessible to a network outside its subnet.

- **`nmap -p- <x.x.x.x>`** to scan all the open ports on an IP address.

  For example, **`nmap -p- 10.1.1.1`**. This scan will report all the open ports on the IP address **`10.1.1.1`**.

  > **NOTE**
  >
  > It may take some time to scan all the ports.

- **`telnet <x.x.x.x> <port>`** to see if telnet is connecting to the IP address on the defined port.

  For example, **`telnet 10.1.1.1 8501`**. This will attempt a connection to **`10.1.1.1`** on port **`8501`**. Since the port is blocked as per **Scenario 3**, the connection attempt should fail.

Linux-based Manager: Frequently asked questions

The following section has frequently asked questions regarding the Linux-based Manager:

1. **What is a Linux-based Manager Appliance?**

   A Linux-based Manager Appliance is a hardware that runs on a pre-installed, hardened MLOS and comes pre-loaded with the Trellix IPS Manager software.

2. **What is MLOS?**

   MLOS is a Trellix proprietary, standardized Linux-based platform on which various Trellix security appliances are built.

3. **What are the advantages of a Linux-based Manager?**

   - The Linux-based Manager Appliance replaces the Windows-based Manager Appliance which is already End of Sale and will be End of Life in 01-April-2023.
   - The Linux-based Manager Appliance is built on MLOS. The MLOS is Trellix proprietary and requires no additional licensing unlike Windows.
   - Easy deployment of the Manager virtual instance in ESXi and KVM environments.

4. **Where do I find the documentation for the Linux-based Manager?**

   You can find the documentation for Linux-based Manager in the following documents:

   - Trellix Intrusion Prevention System 11.1.x Manager-NS-series Release Notes
   - Trellix Intrusion Prevention System 11.1.x Product Guide
   - Trellix Intrusion Prevention System 11.1.x Installation Guide

5. **Do I get to see any performance improvement in a Linux-based Manager when compared to a Windows-based Manager?**

   The performance of a Linux-based Manager is better when compared to a Windows-based Manager.

6. **What is the version of MLOS used in the Linux-based Manager Appliance?**

   Currently, the Linux-based Manager Appliance is pre-installed with MLOS version 3.9.1

7. **Which Trellix IPS Sensor models can a Linux-based Manager manage?**

   The following IPS Sensor models can be managed by a Linux-based Manager:

   - **NS-series**: NS9500 standalone and stack, NS9300, NS9200, NS9100, NS7600, NS7500, NS7350, NS7250, NS7150, NS7300, NS7200, NS7100, NS5200, NS5100, NS3500, NS3200, and NS3100
   - **Virtual IPS**: IPS-VM5000 and IPS VM600

8. **What are the available software versions of a Linux-based Manager/Central Manager?**

   Currently, the Linux-based Manager software versions available are as follows:

   - **10.1**: 10.1.7.65, 10.1.7.66, 10.1.7.66.3,10.1.7.66.11
   - **11.1**: 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

   For the list of compatible Manager and Sensor software versions, refer Manager version and its compatible Sensor software versions.

9. **What are the Sensor software versions that a Linux-based Manager can manage?**

   The Sensor software versions that a Linux-based Manager can manage are as follows:

Sensor models		11.1	10.1
NS-series		11.1.5.2, 11.1.5.22, 11.1.5.44, 1.1.5.56, 11.1.5.57, 11.1.5.72	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, 10.1.5.107, 10.1.5.116, 10.1.5.153, 10.1.5.170, 10.1.5.190, 10.1.5.202, 10.1.5.204
Virtual IPS	IPS-VM600	11.1.7.1, 11.1.7.22, 11.1.7.44, 11.1.7.56, 11.1.7.72	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)
	IPS-VM5000	11.1.7.44, 11.1.7.56, 11.1.7.72	NA

NOTE

A lower version of Linux-based Manager cannot manage a higher version of Sensor. For example, a Linux-based Manager version 10.1.7.61 cannot manage a Sensor running software version 10.1.5.190.

10. **What are the total numbers of Sensors that can be managed by a Linux-based Manager?**

    The Linux-based Manager can manage the same number of Sensors as a Windows-based Manager. The maximum number of Sensors that a Linux-based Manager can manage varies according to the database size, alert rate, and the total traffic inspected by all Sensors attached to the Manager.

11. **Can I install the Linux-based Manager/Central Manager as a virtual instance?**

    You can deploy the Linux-based Manager/Central Manager as a virtual machine in your ESXi and KVM servers. The virtual Manager/Central Manager image can be deployed as a virtual instance of the Manager/Central Manager running on a Linux machine.

12. **Where do I get an OVA and qcow2 images of the Linux-based Manager/Central Manager?**

    The OVA and qcow2 images for a Linux-based Manager/Central Manager is available in the Trellix Download Server.

> **NOTE**
>
> The qcow2 images for the Linux-based Manager/Central Manager is available starting 11.1 Update 4 release.

13. **Where do I get an ISO image of the Linux-based Manager/Central Manager?**

    Trellix does not provide an ISO image of the Linux-based Manager/Central Manager.

    > **NOTE**
    >
    > Trellix recommends you to use the OVA/qcow2 image for Linux-based Manager virtual machine deployment and bootable image shared by the Trellix Support for migrating from Windows-based Manager to Linux-based Manager.

14. **What is Manager shell?**

    Manager shell is the command line interface for the Linux-based Manager. For simplicity of usage and security, the Manager shell is introduced. It allows you to perform various Manager/Central Manager activities.

15. **Which application should I use for SSH connection to the Linux-based Manager CLI?**

    Trellix recommends you to use Tera Term or Bitvise application for SSH connection to the Linux-based Manager CLI.

    > **NOTE**
    >
    > SSH connection to the Linux-based Manager CLI is not supported by Putty application.

16. **What are the credentials for logging into the Manager shell?**

    The login credentials for the Manager shell are as follows:

    For Manager:

    User name: **`admin`**

    Password: **`MLOSnsmApp`**

    For Central Manager:

    Username: **`admin`**

    Password: **`MLOSnscmApp`**

17. **How do I upgrade the Linux-based Manager/Central Manager?**

    You can upgrade your Linux-based Manager/Central Manager using the **`upgrade`** command in the Manager shell. For more information, see [Trellix Intrusion Prevention System Installation Guide].

18. **Where do I get the Linux-based Manager upgrade file?**

    The Linux-based Manager software upgrade file (setup.bin) is available in the Trellix Download Server.

    > **NOTE**
    >
    > You cannot directly download the Linux-based Manager upgrade file (setup.bin) to your Linux-based Manager machine. The upgrade file should be downloaded to a separate machine running SCP or TFTP service in your network.

19. **Are the upgrade files for a Linux-based Manager virtual machine and Manager Appliance same?**

    The upgrade file (setup.bin) is same for the Linux-based Manager virtual machine and Manager Appliance.

20. **How do I take a database backup of a Linux-based Manager?**

    You can take the database backup either using the Manager GUI or Manager shell.

    For collecting the database backup in the Manager shell, execute **`run dbBackup.sh`** command.

    > **NOTE**
    >
    > Trellix recommends you to stop the Manager database service before taking the backup.

21. **What should I do to avoid data corruption when upgrading?**

    Trellix strongly recommends you to take a database backup before an upgrade or migration to avoid data corruption.

22. **How do I access the MariaDB shell?**

    You can access the MariaDB shell by executing **`dbShell`** command in the Manager shell.

    > **NOTE**
    >
    > The default username and password for the MariaDB are **`admin`** and **`admin123`** respectively.

23. **How do I change the database password?**

    You can change the database password by executing **`run passwordchange.sh`** command in the Manager shell.

    > **NOTE**
    >
    > The default database root password is **`root123`**.

24. **How do I access root shell?**

    Trellix recommends you to contact Trellix Support for any information needed regarding root shell.

25. **Can I use `scpToRemote` command to copy files from a Linux-based Manager to a Windows machine?**

    The **`scpToRemote`** command can only be used to copy files to a remote Linux machine.

26. **How do I use InfoCollector utility in the Manager shell?**

    You can the InfoCollector utility in the Manager shell using **`run InfoCollector.sh`** command. You can then copy the InfoCollector logs to a remote machine using **`scpToRemote`** command.

27. **Can I collect the InfoCollector logs using Linux-based Manager UI?**

    You can collect the InfoCollector logs using Manager shell only. But you can collect all logs separately that are collected by InfoCollector tool in the Manager GUI.

28. **What is the use of collect logs command?**

    The collect logs command is used for debugging purpose. It collects all Manager logs. For example, ems.log, emsout.log, emssync.log, initdb.log etc.

29. **What is the difference between the logs collected from InfoCollector utility versus the logs collected from the collect logs command?**

    Collect logs command collects only the logs related to the Manager. InfoCollector utility collects system information, Manager logs, and configuration backup.

30. **Can a Linux-based Manager manage an NTBA Appliance?**

    The Linux-based Manager can manage an NTBA Appliance.

31. **Can I install the Linux-based Manager software on a third-party hardware?**

    Trellix recommends you not to install the Linux-based Manager software on a third-party Linux hardware.

32. **Does Trellix support any other Linux platforms for the Manager software?**

    Currently, a Linux-based Manager software can only be installed in a MLOS.

COPYRIGHT