Trellix Intrusion Prevention System

(NS7500 Quick Start Guide)

This quick start guide explains how to quickly set up and activate your Trellix Intrusion Prevention System NS-series Sensor in in-line mode.

All product documentation referenced in this quick start guide is found on the Trellix Documentation Portal.

The NS7500 Sensor model

Figure 1 Sensor front panel

1 Console port (1)

2 RJ-11 port (1) for fail-open control of two built-in SFP+ ports in G0. This port is used only for passive fail-open mode.

3 SFP+ 1/10 Gigabit Ethernet ports (2). These ports support 1 Gbps (SFP) copper or fiber and 10 Gbps (SFP+) (SR and LR).

4 Two slots for I/O modules (Any combination of the interface modules can be used)

- 8-port SFP/SFP+ 1/10 Gigabit interface module
- 4-port 1/10 Gigabit fiber interface module with built-in fail open
- 6-port RJ45 10/100/1000 Mbps Ethernet interface module with built-in fail open
- 4-port RJ45 100/1000/10000 Mbps Ethernet interface module with built-in fail open

5 Built-in RJ45 10/100/1000 Mbps Ethernet Monitoring ports (8) with internal fail-open

The supported transceiver modules are SFP+ (MM and SM), SFP Fiber (MM and SM) and SFP Copper.

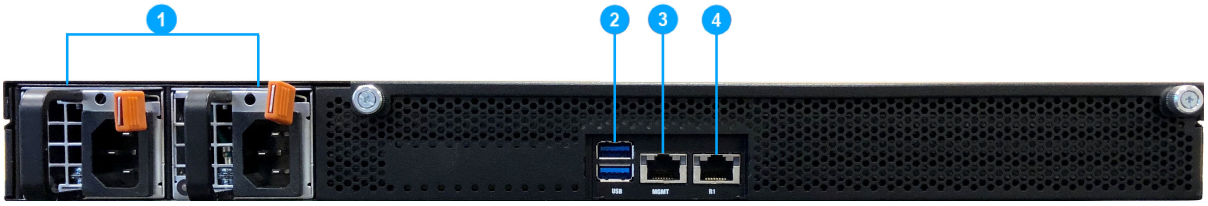


Figure 2 Sensor rear panel

1 Power supply A/B (Pwr A/Pwr B)

2 USB ports (2)

3 RJ-45 1000/10000 Management port (Mgmt) (1)

4 RJ-45 1000/10000 Response port (R1) (1)

1 Verify the contents in the box

The following accessories are shipped in the NS-series Sensor crate:

- Sensor
- Power supply (x2)
- Power cords (Trellix provides a standard and international power cables)
- Set of rack mounting rails
- Printed Quick Start Guide
- Serial Console Cable (DB9-DB9)

2 Verify the hardware and software requirements

Make sure to meet the following hardware requirements. For more information, refer to *Trellix Intrusion Prevention System Installation Guide*.

Windows based Manager application requirements

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

Note

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

	Minimum required	Recommended
Operating system	Any of the following: • Windows Server 2016 Standard Edition English operating system • Windows Server 2016 Standard Edition Japanese operating system • Windows Server 2016 Datacenter Edition English operating system • Windows Server 2016 Datacenter Edition Japanese operating system • Windows Server 2019 Standard Edition English operating system • Windows Server 2019 Standard Edition Japanese operating system • Windows Server 2019 Datacenter Edition English operating system • Windows Server 2019 Datacenter Edition Japanese operating system • Windows Server 2022 Standard Edition English operating system • Windows Server 2022 Standard Edition Japanese operating system • Windows Server 2022 Datacenter Edition English operating system • Windows Server 2022 Datacenter Edition Japanese operating system **Note:** Only x64 architecture is supported.	Windows Server 2022 Datacenter Edition operating system
Memory	16 GB **Note:** Supports up to 10 million alerts in Solr	>=32 GB **Note:** Supports up to 20 million alerts in Solr
CPU	Server model processor, such as Intel Xeon	Same
Disk space	300 GB	500 GB or more

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

Table 1 VMware ESX server requirements for Windows Operating System

Component	Supported
Virtualization software	• ESXi 7.0 Update 3 • ESXi 8.0 **Note:** Hyperthreading should be available.

Linux based Manager application requirements

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

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

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

Table 2 VMware ESX server requirements for MLOS

Component	Supported
Virtualization software	• ESXi 7.0 Update 3 • ESXi 8.0 **Note:** Hyperthreading should be available.

Manager client system requirements

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

	Minimum	Recommended
Operating system	Windows 10, English or Japanese **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

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

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

Mac operating system	Browser
Ventura	Safari 16 or later

Install the following software:

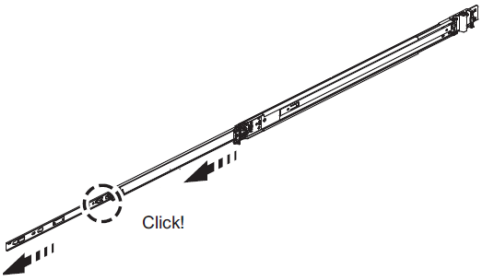
- Manager image
- Sensor image
- Signature set

3 Install the slide rails

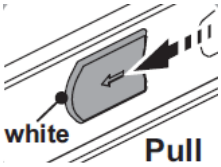
Follow this procedure to assemble the slide rails and position the Sensor on it.

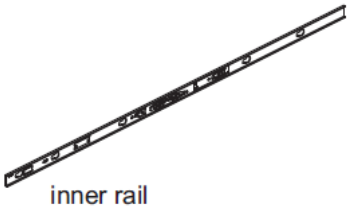
a Disassemble the inner slide rails from the rail assemblies.

a Pull the inner rail out.



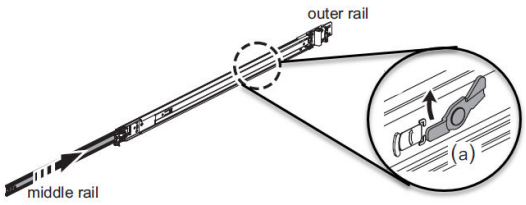
b Click and pull the white tab (lock on inner rail) forward to disconnect inner rail from the middle rail.

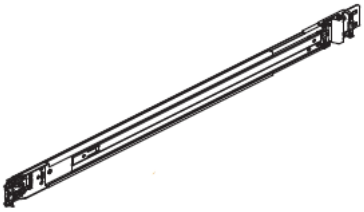




The Inner rail is disconnected.

c Push tab (a) to slide the middle rail back into the outer rail.



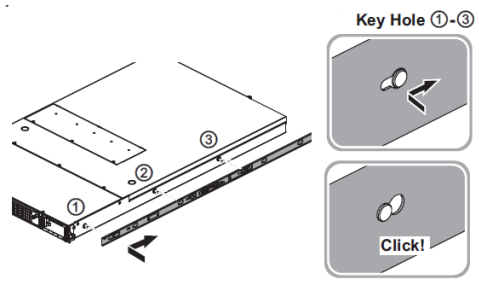


The middle rail is pushed back into the outer rail.

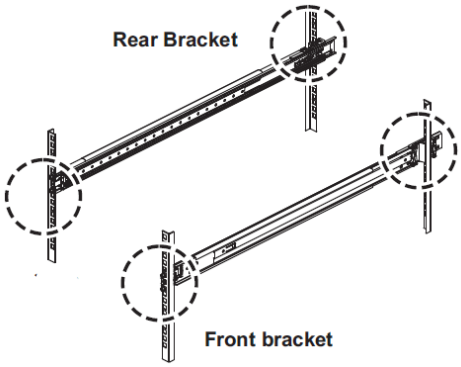
b Mount the inner rail onto the chassis unit.

a Place each inner rail on both sides of the chassis unit. Position the three key holes of the inner rails with the mounting holes on the chassis unit.

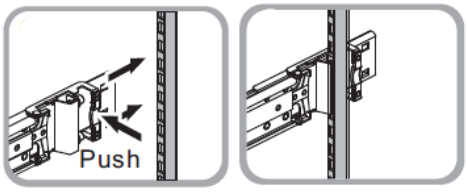
b Slide the rails forward to lock it.



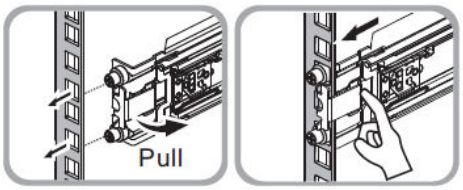
c Mount the outer slide rails/brackets to the rack posts.



a Install the rear brackets to the rack. Push the latch forward to ensure the latch is completely installed in the rack posts.



b Install the front brackets to the rack. Pull the front securing latch bracket and insert the pegs into the rack holes. Push the securing latch onto the rack post.



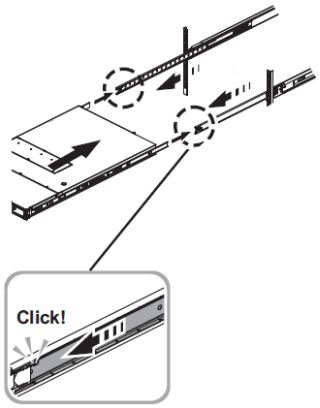
d Mount the chassis unit into the rack.

a Pull the middle rail out, extend it until the lock position.

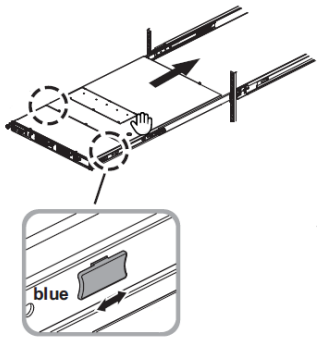
Note

Ensure ball bearing retainer is located at the front of the middle rail.

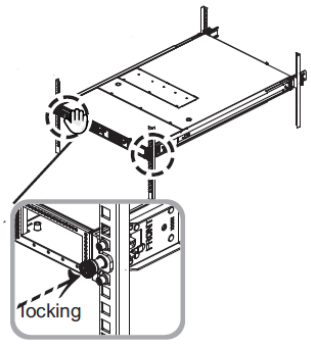
b Insert the chassis unit into the middle rails.



c Pull or push the blue release tab on both sides and continue to push the chassis unit until fully closed.



d Secure the chassis unit by locking it. Add thumb screws on both the sides of the rack post.



4 Install the interface modules

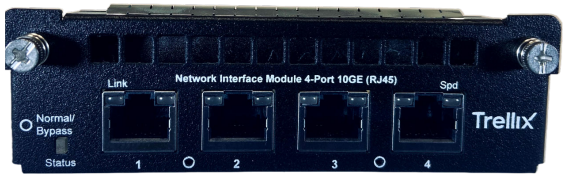
You can purchase the following interface modules and insert them into the relevant slots on your NS-series Sensor.

- 8-port SFP/SFP+ 1/10 Gigabit interface module
- 4-port 1/10 Gigabit fiber interface module with built-in fail open

- 6-port RJ45 10/100/1000 Mbps Ethernet interface module with built-in fail open
- 4-port RJ45 100/1000/10000 Mbps Ethernet interface module with built-in fail open

a Remove the module from its protective packaging.

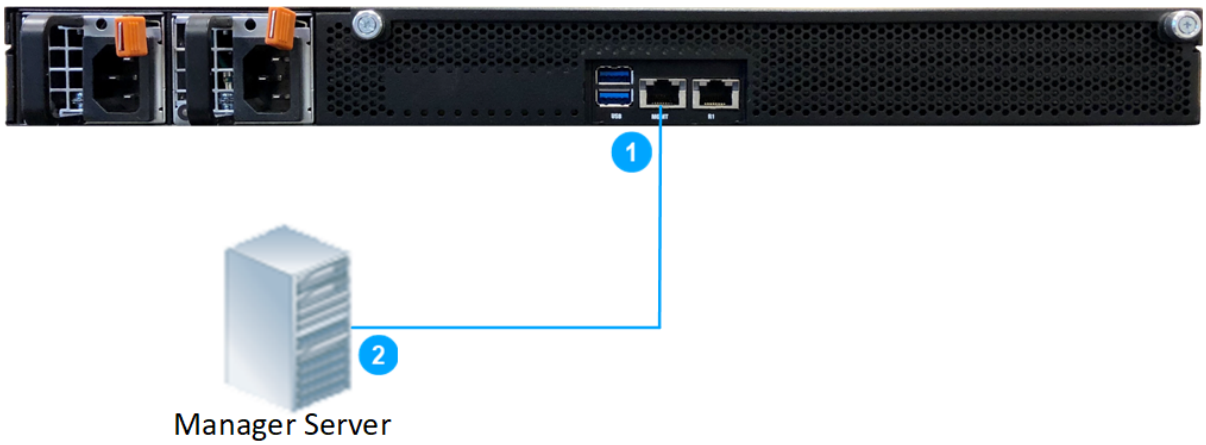
b Grip the sides of the module with your thumb and fore-finger and insert the module into the slot.



c Drive in the screws fixed on the sides of the module to attach it to the Sensor.

5 Cable the Management and Console ports

a On the rear panel of the NS7500 Sensor, plug a RJ-45 cable in the Management port (labeled MGMT, for example, 1).



b Plug the other end of the cable into the network device connected to your Manager server (for example, 2).

c On the front panel of the NS7500 Sensor, plug the DB9 Console cable(s) into the Console port (labeled Console).

d Connect the other end of the Console port cable directly to a COM port of the PC or terminal server you will be using to configure the Sensor (for example, a PC running correctly configured Windows Hyperterminal software). You must connect directly to the console for initial configuration; you cannot configure the Sensor remotely.

Terminal servers are provided for console access.

The required settings for Hyperterminal are as follows:

- Baud rate: 115200
- Number of Bits: 8
- Parity: None
- Stop Bits: 1
- Control Flow: None

e Plug one end of the power cable into the power inlet and plug the other end into a power source. The Sensor ships with standard US power and international cables.

Note

The NS-series Sensor does not have a power switch; you need to only plug the power cable into a power source.

6 Cable the Monitoring ports

This procedure describes how to cable a Sensor to run in In-line mode.

a Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports labeled x (for example, 1).

b Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports labeled y (for example, 2).

c Connect the other end of each cable to the network devices that you want to monitor. For example, if you plan to monitor traffic between a switch and a router, connect the cable connected to 1 to the router (3) and the one connected to 2 to the switch (4).

7 Install the Manager Software

Following steps briefly explain the Manager installation:

Note

You must have administrator privileges on the target Windows or Linux server to install the Manager software.

Note

MariaDB is included with the Manager and is installed (embedded) automatically on your target Windows or Linux server during this process.

a Prepare the system according to the requirements outlined in *Trellix Intrusion Prevention System Installation Guide*.

b Close all open applications.

c Go to Trellix Download Server (`https://www.trellix.com/en-us/downloads/my-products.html`).

d Log on using your `Grant Number` and registered `Email Address`.

The **Find Products** page opens.

e In the **Category** filter, select **Network Security**.

f Click on the Manager version required.

The **Available Downloads** page opens.

g In the **Type** filter, select **Installation**.

The Manager installation files available for download are listed.

h Click on the required Manager installation file and the download starts.

i Refer to *Trellix Intrusion Prevention System Installation Guide* for detailed procedure to install the Manager application.

8 License requirement for NS7500 Sensors

The NS7500 Sensor requires a license to activate the baseline throughput. You must first purchase a license to enable traffic inspection in the NS7500 Sensor. To obtain a license, contact **Trellix Sales**.

The license is provided as a .zip or .jar file. The Manager supports both formats. The license procured contains the details of the throughput for the Sensor.

The table below shows the licenses available for the NS7500 Sensors:

License SKUs	Throughput	No of Sensors
NS7500-3GBPS	3 Gbps	1 NS7500 Sensor
NS7500-5GBPS	5 Gbps	1 NS7500 Sensor
NS7500-7.5GBPS	7.5 Gbps	1 NS7500 Sensor

You can upload the license from the **Licenses** page in the Manager. In the Manager, go to **Manager** | **<Admin Domain>** | **Setup** | **Licenses**.

For more information on license, refer to *Trellix Intrusion Prevention System NS-series Sensor Product Guide*.

9 Add a Sensor to the Manager

After a Sensor is configured with a name and shared key value, you can add the Sensor to the Manager on the **Sensors** tab of the **Device Manager** page.

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

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

a Log on to the Manager using the default user name `(admin)` and password `(admin123)`.

b Go to **Devices** | **<Admin Domain Name>** | **Global** | **Device Manager**.

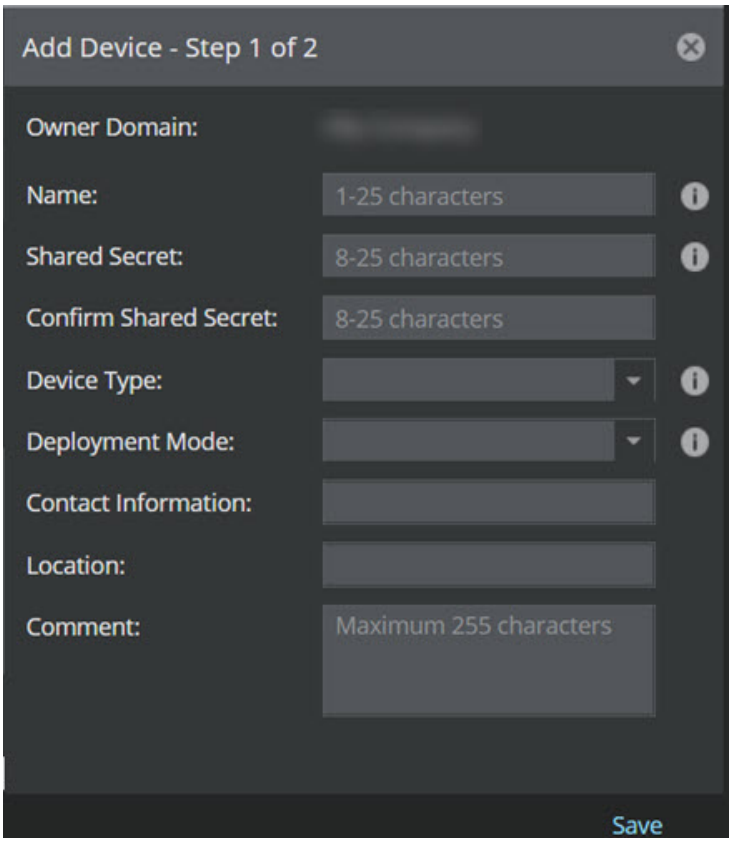
The **Device Manager** page is displayed.

c Select the **Sensors** tab and then click +.

Note

You do not require a license file to enable IPS on NS-series Sensors.

The **Add Devices - Step 1 of 2** panel is displayed.



d Enter the following mandatory information in the appropriate fields:

1) **Name** — The Sensor name must begin with a letter. The maximum length of the name is 25 characters.

2) **Shared Secret** — The shared secret must be a minimum of 8 characters and maximum of 25 characters in length. The key cannot start with an exclamation mark nor can have any spaces. The parameters that you can use to define the key are listed below:

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

Retype the password in **Confirm Shared Secret**.

Note

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

3) **Device Type** — Specifies the type of device to be added. Select **IPS Sensor**.

4) **Deployment Mode** — Select **Direct** or **Indirect**.

Note

Selecting **Direct** enables online Sensor update. **Direct** is the default mode.

5) **Contact Information** — (Optional) Type the contact information.

6) **Location** — (Optional) Type the location.

7) **Comment** — (Optional) Type the comment.

e Click **Save**.

The added Sensor is displayed on the **Sensors** tab of **Device Manager** page.

10 Configure Sensor information

Configure the Sensor with the network information, a name, and the shared secret key that the Sensor uses to establish secure communication with the Manager. Use the name and key values you set in *Add the Sensor to the Manager* section.

Tip

You must have physical access to the Sensor when you configure a Sensor for the first time.

At any time during configuration, you can type a question mark (`?`) to get help on the Sensor CLI commands. Type `commands` for a list of all commands.

a Log in to the Sensor using the terminal connected to the Console port.

b At the prompt, log in using the default Sensor username `admin` and password `admin123`.

c (Optional, but recommended) Change the Sensor password. At the prompt, type `passwd`. The Sensor prompts you to enter the new password and asks you for the old password.

Note

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

d Set the name of the Sensor.

Tip

You can enter the `setup` command at the prompt which will automatically prompt you to provide the information shown in the subsequent steps of this section. Or, you can use the `set` command instead. If you use the `set` command, you must manually enter the complete command syntax as shown in the subsequent steps of this section.

Type `set sensor name <word>` at the prompt.

Example: `set sensor name HR_sensor1`

Note

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

e If the Sensor is not on the same network as the Manager, set the address of the default gateway. Type `set sensor gateway <A.B.C.D>` at the prompt.

Example: `set sensor gateway 192.168.3.68`

f Set the IP address of the Manager server. Type `set manager ip <A.B.C.D>` at the prompt.

Example: `set manager ip 192.168.2.8`

g Set the IP address and subnet mask of the Sensor. Type `set sensor ip <A.B.C.D> <E.F.G.H>` at the prompt.

Example: `set sensor ip 192.168.2.12 255.255.255.0`

Note

Specify an IP address using four octets separated by periods: X.X.X.X, where X is a number between 0 and 255, followed by a subnet mask in the same format.

h If prompted, reboot the Sensor. Type `reboot`

Note

The Sensor can take up to five minutes to complete its reboot.

i Ping the Manager from the Sensor to determine if your configuration settings to this point have successfully established the Sensor on the network. At the prompt, type the following command:

`ping <manager IP address>`

If the ping is successful, continue with the following steps. If not, type `show` to verify your configuration settings and check if the information is correct.

j Set the shared secret key value for the Sensor. At the prompt, type the following command:

`set sensor sharedsecretkey`

The Sensor then prompts you to enter and, subsequently, confirm the shared secret key value.

Note

This value is used to establish a trust relationship between the Sensor and the Manager. The secret key value can be between 8 and 25 characters of any ASCII text. The shared key value is case-sensitive. Make sure the value matches the shared secret key value you provided in the Manager interface while adding the Sensor.

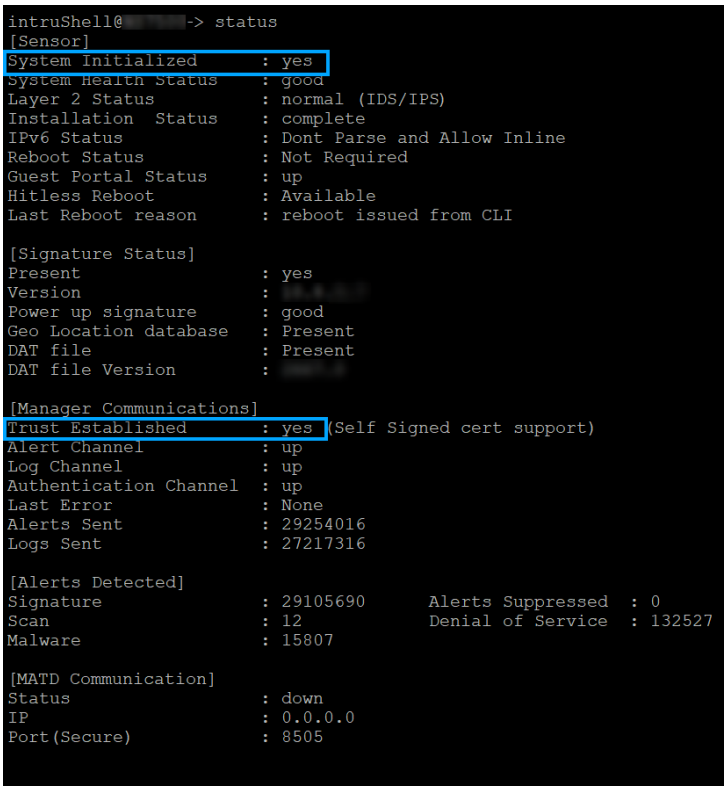
k Type `show` to verify the configuration information. Check that all information is correct.

l Type `exit` to exit the session.

11 Verify successful installation

a Type `status` in the Sensor CLI.

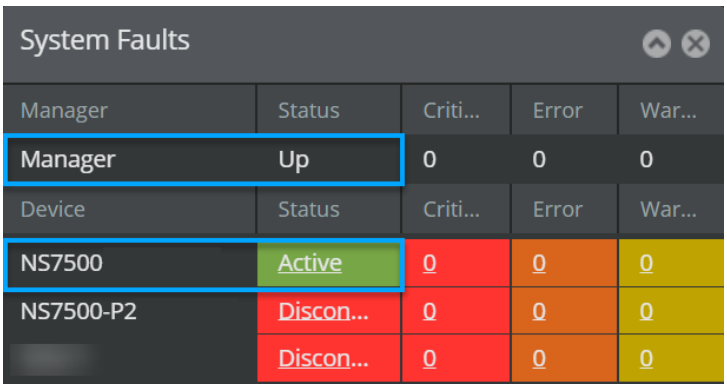
The status report appears.



The Sensor parameter `System Initialized` should be `yes`, and for Manager communications `Trust Established` should be `yes`.

b From the Manager **Dashboard**, view the Manager status in the **System Faults** monitor.

The Manager status displays as **Up** and Sensor status is **Active**.

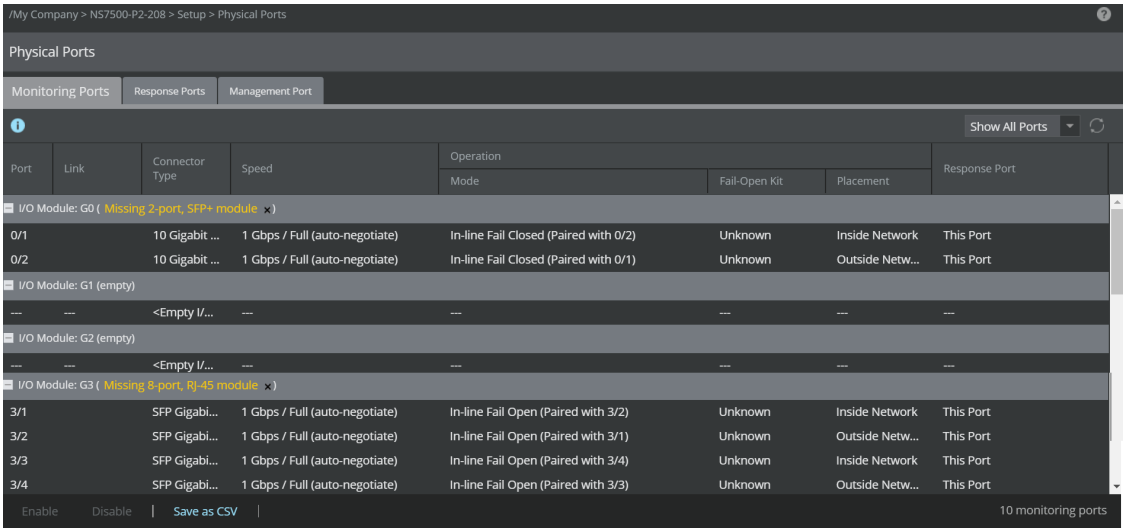


c From the Manager, click **Devices** | **<Admin Domain>** | **Devices** | **Setup** | **Physical Ports** to view the port details of the Sensor.

To view port settings, select the port on the Sensor that you cabled. Ensure that your port settings match the cabling. For example, if port 1 is cabled for inline mode, the mode of operation in the port setting should be inline mode.

Note

For more information on port settings, see the chapter *Configuring the monitoring and response ports of a Sensor* in *Trellix Intrusion Prevention System Product Guide*.



d A policy named **Default Prevention** is active upon the addition of the Sensor. To view this policy, select **Policy** | **<Admin Domain>** | **Intrusion Prevention** | **Policy Types** | **IPS Policies**.

The **Default Prevention** policy contains attacks already configured with a "blocking" Sensor response action. If any attack in the policy is triggered, the Sensor automatically blocks the attack. To tune this or any other Trellix-provided policies, you can clone the policy and then customize it as described in *Trellix Intrusion Prevention System Product Guide*.

12 You're up and running!

Your Sensor is actively monitoring connected segments and communicating with the Manager for administration and management operations.

a For detailed usage instructions, see *Trellix Intrusion Prevention System Product Guide*, or click in the upper-right corner of each window in the Manager.

b Go to **Analysis** | **<Admin Domain>** | **Attack Log** to view alert statistics as attacks are detected. A summary of alerts is displayed in the **Attack Severity Summary** monitor of the Manager **Dashboard** page.

c Having problems? Check *Trellix Intrusion Prevention System Product Guide* for troubleshooting information.

d Most deployment problems stem from configuration mismatches between the Sensor and the network devices to which it is connected. Check your duplex and auto-negotiation settings on both devices to ensure they are synchronized.

If you need to contact Technical Support, go to https://www.trellix.com/en-us/support.html.

700-5484H30

Trellix