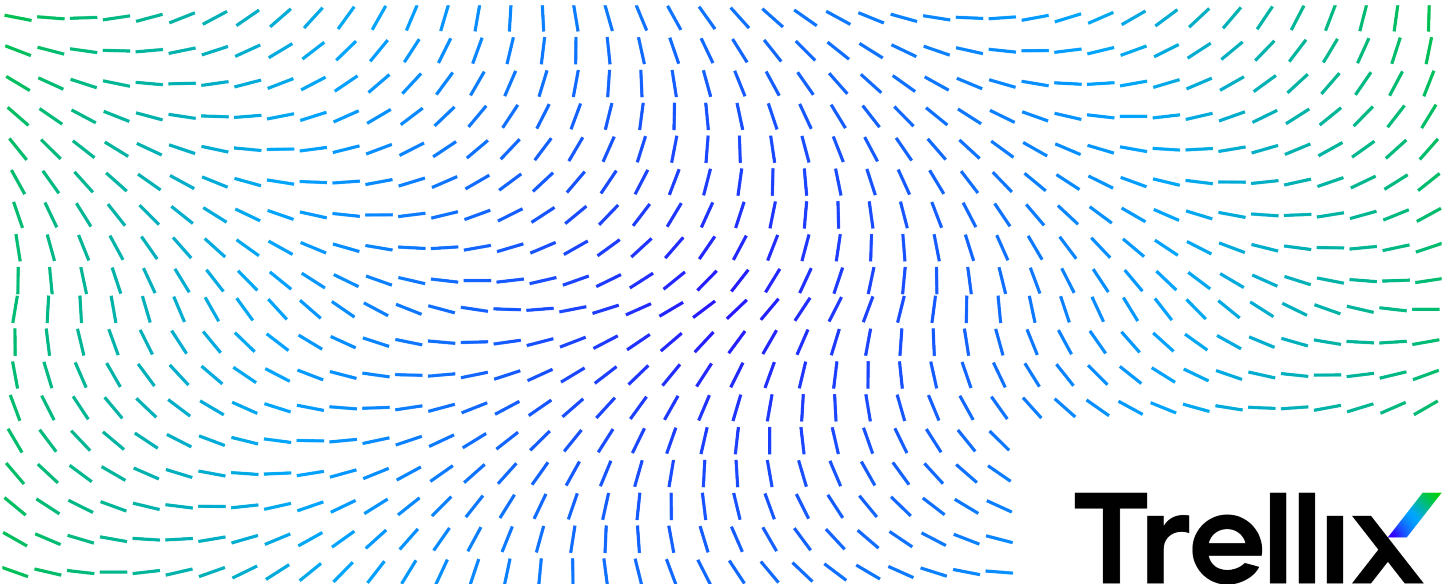


# Trellix Intrusion Prevention System NS-series Sensor Product Guide



# Contents

---

<b>NS9500 Sensors</b> .....	<b>16</b>
About Sensors.....	16
Functions of an NS-series Sensor.....	16
Deployment of an NS-series Sensor.....	16
NS-series physical description.....	17
Components of an NS-series Sensor.....	17
Sensor LEDs.....	18
Before you install.....	20
Usage restrictions.....	21
Safety measures.....	21
About fiber-optic ports.....	22
Contents of the box.....	22
Unpack the Sensor.....	23
Setting up the Sensor.....	23
Setup overview.....	23
How to position the Sensor.....	23
Install the slide rails and rack mount the Sensor.....	24
NS-series interface modules.....	28
2-port QSFP28 100 Gigabit Network Interface Module.....	28
2-port QSFP+ 40 Gigabit Network Interface Module.....	29
2-port 100/40 Gigabit SR MTP/MPO passive fail-open interface module.....	29
4-port QSFP+ 40 Gigabit Network Interface Module.....	30
4-port 10/1 GigE SM 8.5 $\mu$ m with internal fail-open Network Interface Module.....	30
4-port 10/1 GigE MM 50 $\mu$ m with internal fail-open Network Interface Module.....	31

4-port 10/1 GigE MM 62.5 $\mu$ m with internal fail-open Network Interface Module. . . . .	31
4-port RJ-45 10 Gbps/1 Gbps/100 Mbps Network Interface Module. . . . .	32
6-port RJ-45 10/100/1000 Mbps Network Interface module. . . . .	33
8-port SFP/SFP+ 1/10 Gigabit Network Interface Module. . . . .	33
Installation of the interface module. . . . .	34
Install the interface module during a fresh installation of the Sensor. . . . .	34
Install the interface module on an up and running Sensor. . . . .	35
Remove an interface module. . . . .	35
Small form-factor pluggable transceiver modules. . . . .	35
SFP transceiver modules. . . . .	36
SFP+ transceiver modules. . . . .	36
QSFP+ transceiver modules. . . . .	37
QSFP28 transceiver modules. . . . .	38
Install a transceiver module. . . . .	39
Remove a transceiver module. . . . .	39
Attaching cables to the Sensor. . . . .	40
Connect the cable to the Console port. . . . .	40
Connect the cable to the Response port. . . . .	41
Connect the cable to the Management port. . . . .	41
About connecting cables to the Monitoring ports. . . . .	41
How to use peer ports. . . . .	41
Cable types for routers, switches, hubs, and computers. . . . .	43
Connect the cables for in-line mode. . . . .	43
Connect the cables for tap mode. . . . .	43
Connect the cables for SPAN or hub mode. . . . .	44
Connect the cable for standalone Sensor failover. . . . .	44
Connect the cables for Sensor Fail-Open. . . . .	45
Turning the Sensor on and off. . . . .	46
License requirement for NS9500 Sensors. . . . .	46
License requirement for NS9500 Sensor failover. . . . .	48

Managing licenses for NS9500 Sensors. ....	50
Add license to the Manager. ....	52
Assign a license to a Sensor. ....	53
Unassign a license from a Sensor. ....	55
Upgrade an existing capacity license. ....	56
Remove a license from the Manager. ....	60
Stacking NS9500 Sensors. ....	61
Considerations for NS9500 Sensor stack. ....	61
Cable the Sensors in a standalone stack. ....	62
Add a stack to the Manager. ....	63
Configure Sensor information. ....	66
Considerations for failover in stacked Sensors. ....	68
Cable the Sensors in a stack for high availability. ....	69
Scenarios for stacked NS9500 Sensors. ....	70
Configure the Sensor and Manager for deployment. ....	73
Install the Manager Software. ....	73
Add the Sensor to the Manager. ....	74
Configure Sensor information. ....	76
Verify successful installation. ....	78
You're up and running!. ....	80
Troubleshooting the Sensor. ....	80
Sensor technical specifications. ....	81

**NS9x00 Sensors. .... 84**

About Sensors. ....	84
Functions of an NS-series Sensor. ....	84
Deployment of an NS-series Sensor. ....	85
NS-series physical description. ....	85
Components of an NS-series Sensor. ....	85
Sensor LEDs. ....	91
Before you install. ....	93

Usage restrictions. . . . .	94
Safety measures. . . . .	94
About fiber-optic ports. . . . .	95
Contents of the box. . . . .	95
Unpack the Sensor. . . . .	95
Setting up the Sensor. . . . .	96
Setup overview. . . . .	96
How to position the Sensor. . . . .	96
Install the slide rails and rack mount the Sensor. . . . .	96
Redundant power supply. . . . .	100
Install a new power supply. . . . .	100
Remove the power supply. . . . .	101
NS-series Network Interface modules. . . . .	101
Installation of the interface module. . . . .	102
Install the interface module during a fresh installation of the Sensor. . . . .	102
Install the interface module on an up and running Sensor. . . . .	103
Remove an interface module. . . . .	103
Small form-factor pluggable transceiver modules. . . . .	103
Install a transceiver module. . . . .	104
Remove a transceiver module. . . . .	105
Attaching cables to the Sensor. . . . .	105
Connect the cable to the Console port. . . . .	105
Connect the cable to the Auxiliary port. . . . .	106
Connect the cable to the Response port. . . . .	106
Connect the cable to the Management port. . . . .	106
Connect the cables to the Interconnect ports. . . . .	107
About connecting cables to the Monitoring ports. . . . .	107
How to use peer ports. . . . .	107
Cable types for routers, switches, hubs and computers. . . . .	109
Connect the cables for in-line mode. . . . .	109

Connect the cables for tap mode. ....	110
Port Clustering for an NS9300 Sensor in tap mode. ....	110
Connect the cables for SPAN or hub mode. ....	113
Connect the cables for Sensor Fail-Open. ....	113
Connect the cable for Sensor failover. ....	114
Turning the Sensor on and off. ....	115
Configure the Sensor and Manager for deployment. ....	115
Install the Manager Software. ....	116
Add the Sensor to the Manager. ....	116
Configure Sensor information. ....	118
Verify successful installation. ....	120
You're up and running!. ....	122
Troubleshooting the Sensor. ....	122
Sensor technical specifications. ....	123

**NS7500 Sensor. .... 126**

About Sensors. ....	126
Functions of an NS-series Sensor. ....	126
Deployment of an NS-series Sensor. ....	126
NS-series physical description. ....	127
Components of an NS-series Sensor. ....	127
Sensor LEDs. ....	128
Before you install. ....	130
Usage restrictions. ....	131
Safety measures. ....	131
About fiber-optic ports. ....	132
Contents of the box. ....	132
Unpack the Sensor. ....	132
Setting up the Sensor. ....	133
Setup overview. ....	133
How to position the Sensor. ....	133

Install the slide rails and rack mount the Sensor. ....	133
NS-series interface modules. ....	137
4-port 10/1 GigE SM 8.5 $\mu$ m with internal fail-open Network Interface Module. ....	138
4-port 10/1 GigE MM 50 $\mu$ m with internal fail-open Network Interface Module. ....	138
4-port 10/1 GigE MM 62.5 $\mu$ m with internal fail-open Network Interface Module. ....	139
4-port RJ-45 10 Gbps/1 Gbps/100 Mbps with internal fail-open Network Interface Module. ....	139
6-port RJ-45 1 Gbps/100 Mbps/10 Mbps with internal fail-open Network Interface Module. ....	140
8-port SFP/SFP+ 1/10 Gigabit Network Interface Module. ....	141
Installation of the interface module. ....	141
Install the interface module during a fresh installation of the Sensor. ....	141
Install the interface module on an up and running Sensor. ....	142
Remove an interface module. ....	142
Small form-factor pluggable transceiver modules. ....	143
SFP transceiver modules. ....	143
SFP+ transceiver modules. ....	144
Install a transceiver module. ....	144
Remove a transceiver module. ....	145
Attaching cables to the Sensor. ....	145
Connect the cable to the Console port. ....	146
Connect the cable to the Response port. ....	146
Connect the cable to the Management port. ....	147
About connecting cables to the Monitoring ports. ....	147
How to use peer ports. ....	147
Cable types for routers, switches, hubs, and computers. ....	148
Connect the cables for in-line mode. ....	148
Connect the cables for tap mode. ....	149
Connect the cables for SPAN or hub mode. ....	150
Connect the cable for Sensor failover. ....	150
Connect the cables for Sensor Fail-Open. ....	151
Turning the Sensor on and off. ....	152

License requirement for NS7500 Sensors. ....	153
License requirement for NS7500 Sensor failover. ....	154
Managing licenses for NS7500 Sensors. ....	154
Add license to the Manager. ....	157
Assign a license to a Sensor. ....	158
Unassign a license from a Sensor. ....	159
Upgrade an existing capacity license. ....	160
Remove a license from the Manager. ....	163
Troubleshooting the Sensor. ....	164
Sensor technical specifications. ....	165
<b>NS7x50 Sensors. ....</b>	<b>167</b>
About Sensors. ....	167
Functions of an NS-series Sensor. ....	167
Deployment of an NS-series Sensor. ....	168
NS7x50 Sensor physical description. ....	168
Components of an NS7x50 Sensor. ....	168
Sensor LEDs. ....	171
Before you install. ....	173
Usage restrictions. ....	173
Safety measures. ....	174
About fiber-optic ports. ....	174
Contents of the box. ....	175
Unpack the Sensor. ....	175
Setting up the Sensor. ....	176
Setup overview. ....	176
How to position the Sensor. ....	176
Install the slide rails and rack-mount the Sensor. ....	176
Redundant power supply. ....	180
Install a new power supply. ....	181
Remove the power supply. ....	182



NS7x50 Network Interface modules. . . . .	182
Installation of the Interface Module. . . . .	182
Install the interface module during a fresh installation of the Sensor. . . . .	183
Install the interface module on an up and running Sensor. . . . .	183
Remove an Interface Module. . . . .	184
Small form-factor pluggable transceiver modules. . . . .	184
Install a transceiver module. . . . .	185
Remove a transceiver module. . . . .	185
Attaching cables to the Sensor. . . . .	186
Connect the cable to the Console port. . . . .	186
Connect the cable to the Response port. . . . .	187
Connect the cable to the Management port. . . . .	187
About connecting cables to the Monitoring ports. . . . .	187
How to use peer ports. . . . .	188
Cable types for routers, switches, hubs, and computers. . . . .	189
Connect the cables for in-line mode. . . . .	189
Connect the cables for tap mode. . . . .	190
Connect the cables for SPAN or hub mode. . . . .	190
Connect the cables for Sensor Fail-Open. . . . .	190
Connect the cable for Sensor failover. . . . .	192
Turning the Sensor on and off. . . . .	193
Troubleshooting the Sensor. . . . .	193
Sensor technical specifications. . . . .	194

**NS7x00 Sensors. . . . . 197**

About Sensors. . . . .	197
Functions of an NS-series Sensor. . . . .	197
Deployment of an NS-series Sensor. . . . .	198
NS7x00 Sensor physical description. . . . .	198
Components of an NS7x00 Sensor. . . . .	198
Sensor LEDs. . . . .	201

Before you install. . . . .	203
Usage restrictions. . . . .	203
Safety measures. . . . .	204
About fiber-optic ports. . . . .	204
Contents of the box. . . . .	205
Unpack the Sensor. . . . .	205
Setting up the Sensor. . . . .	206
Setup overview. . . . .	206
How to position the Sensor. . . . .	206
Install the slide rails and rack-mount the Sensor. . . . .	206
Redundant power supply. . . . .	209
Install a new power supply. . . . .	209
Remove the power supply. . . . .	210
NS7x00 Network Interface modules. . . . .	210
Installation of the Interface Module. . . . .	211
Install the interface module during a fresh installation of the Sensor. . . . .	211
Install the interface module on an up and running Sensor. . . . .	212
Remove an Interface Module. . . . .	212
Small form-factor pluggable transceiver modules. . . . .	213
Install a transceiver module. . . . .	213
Remove a transceiver module. . . . .	214
Attaching cables to the Sensor. . . . .	214
Connect the cable to the Console port. . . . .	214
Connect the cable to the Response port. . . . .	215
Connect the cable to the Management port. . . . .	216
About connecting cables to the Monitoring ports. . . . .	216
How to use peer ports. . . . .	216
Cable types for routers switches hubs and computers. . . . .	218
Connect the cables for in-line mode. . . . .	218
Connect the cables for tap mode. . . . .	218

Connect the cables for SPAN or hub mode. ....	219
Connect the cables for Sensor Fail-Open. ....	219
Connect the cable for Sensor failover. ....	220
Turning the Sensor on and off. ....	221
Configure the Sensor and Manager for deployment. ....	222
Install the Manager Software. ....	222
Add the Sensor to the Manager. ....	223
Configure Sensor information. ....	224
Verify successful installation. ....	226
You're up and running!. ....	228
Troubleshooting the Sensor. ....	229
Sensor technical specifications. ....	230

## **NS5x00 Sensors. .... 232**

About Sensors. ....	232
Functions of NS-series Sensors. ....	232
Deployment of NS-series Sensors. ....	233
NS5x00 Sensor physical description. ....	233
Components of an NS5x00 Sensor. ....	233
Sensor LEDs. ....	236
Before you install. ....	238
Usage restrictions. ....	238
Safety measures. ....	238
About fiber-optic ports. ....	239
Contents of the box. ....	239
Unpack the Sensor. ....	240
Setting up the Sensor. ....	240
Setup overview. ....	240
How to position the Sensor. ....	240
Install the slide rails and rack-mount the Sensor. ....	241
Redundant power supply. ....	243

Install a new power supply. . . . .	244
Remove the power supply. . . . .	245
Small form-factor pluggable transceiver modules. . . . .	245
Install a transceiver module. . . . .	246
Remove a transceiver module. . . . .	247
Attaching cables to the Sensor. . . . .	247
Connect the cable to the Console port. . . . .	247
Connect the cable to the Response port. . . . .	248
Connect the cable to the Management port. . . . .	248
About connecting cables to the Monitoring ports. . . . .	249
How to use peer ports. . . . .	249
Cable types for routers, switches, hubs, and computers. . . . .	250
Connect the cables for in-line mode. . . . .	250
Connect the cables for tap mode. . . . .	251
Connect the cables for SPAN or hub mode. . . . .	251
Connect the cables for Sensor Fail-Open. . . . .	252
Connect the cable for Sensor failover. . . . .	253
Turning the Sensor on and off. . . . .	253
Configure the Sensor and Manager for deployment. . . . .	254
Install the Manager Software. . . . .	254
Add the Sensor to the Manager. . . . .	255
Configure Sensor information. . . . .	256
Verify successful installation. . . . .	258
You're up and running!. . . . .	260
Troubleshooting the Sensor. . . . .	261
Sensor technical specifications. . . . .	262

**NS3500 Sensors. . . . . 264**

About Sensors. . . . .	264
Functions of NS-series Sensors. . . . .	264
Deployment of NS-series Sensors. . . . .	264

NS3500 Sensor physical description. . . . .	265
Components of an NS3500 Sensor. . . . .	265
Sensor LEDs. . . . .	267
Before you install. . . . .	269
Usage restrictions. . . . .	269
Safety measures. . . . .	269
Contents of the box. . . . .	270
Unpack the Sensor. . . . .	270
Setting up the Sensor. . . . .	271
Setup overview. . . . .	271
How to position the Sensor. . . . .	271
Attaching cables to the Sensor. . . . .	271
Connect the cable to the Console port. . . . .	271
Connect the cable to the Management port. . . . .	272
About connecting cables to the Monitoring ports. . . . .	273
Cable types for routers, switches, hubs, and computers. . . . .	273
Connect the cables for in-line mode. . . . .	274
Connect the cables for tap mode. . . . .	274
Connect the cables for SPAN or hub mode. . . . .	275
Turning the Sensor on and off. . . . .	275
Managing licenses for NS3500 Sensors. . . . .	275
Add license to the Manager. . . . .	277
Assign a license to a Sensor. . . . .	278
Unassign a license from a Sensor. . . . .	280
Remove a license from the Manager. . . . .	281
Troubleshooting the Sensor. . . . .	281
Sensor technical specifications. . . . .	282

**NS3x00 Sensors. . . . . 285**

About Sensors. . . . .	285
Functions of NS-series Sensors. . . . .	285

Deployment of NS-series Sensors.....	286
NS3x00 Sensor physical description.....	286
Components of an NS3x00 Sensor.....	286
Sensor LEDs.....	288
Before you install.....	290
Usage restrictions.....	290
Safety measures.....	290
Contents of the box.....	291
Unpack the Sensor.....	291
Setting up the Sensor.....	291
Setup overview.....	291
How to position the Sensor.....	292
Install the Sensor.....	292
Attaching cables to the Sensor.....	293
Connect the cable to the Console port.....	293
Connect the cable to the Response port.....	294
Connect the cable to the Management port.....	294
About connecting cables to the Monitoring ports.....	295
How to use peer ports.....	295
Cable types for routers, switches, hubs, and computers.....	296
Connect the cables for in-line mode.....	296
Connect the cables for tap mode.....	297
Connect the cables for SPAN or hub mode.....	297
Connect the cables for Sensor Fail-Open.....	297
Connect the cable for Sensor failover.....	298
Turning the Sensor on and off.....	299
Configure the Sensor and Manager for deployment.....	299
Install the Manager Software.....	299
Add the Sensor to the Manager.....	300
Configure Sensor information.....	302

Verify successful installation. ....	304
You're up and running! .....	306
Troubleshooting the Sensor. ....	306
Sensor technical specifications. ....	307

# NS9500 Sensors

:

## About Sensors

Trellix Intrusion Prevention System Sensors are high-performance, scalable, and flexible content processing appliances built for the accurate detection and prevention of:

- Network intrusions
- Network misuse
- Distributed Denial-of-Service (DDoS) attacks

Trellix Intrusion Prevention System Sensors are specifically designed to handle traffic at wire speed, efficiently inspect and detect intrusions with a high degree of accuracy, and flexible enough to adapt to the security needs of any enterprise environment. When deployed at key network access points, the Sensor provides real-time traffic monitoring to detect malicious activity and respond to the malicious activity as configured by the administrator.

After you deploy a Sensor successfully, you configure and manage it using the Trellix Intrusion Prevention System Manager. The process of configuring a Sensor and establishing communication with the Manager is described in subsequent chapters of this guide. For the details about the Trellix IPS Manager, see the *Manager Administration* section in *Trellix Intrusion Prevention System Product Guide*.

:

## Functions of an NS-series Sensor

The NS-series Sensors are a third-generation hardware platform for Trellix IPS Sensors designed for high bandwidth links to offer Next Generation IPS (NGIPS) capability and provide high aggregate throughput across various Sensor models. The NS9500 Sensor is a 1RU unit providing an aggregate throughput up to 30 Gbps.

The primary function of an IPS Sensor is to analyze traffic on selected network segments and to respond when an attack is detected. The Sensor examines the header and data portion of every network packet, looking for patterns and behavior in the network traffic that indicate malicious activity. The Sensor examines packets according to user-configured policies, or rule sets, which determine what attacks to watch for, and how to respond with countermeasures if an attack is detected.

If an attack is detected, a Sensor responds according to its configured policy. Sensor can perform many types of attack responses, including generating alerts and packet logs, resetting TCP connections, "scrubbing" malicious packets, and even blocking attack packets entirely before they reach the intended target.

:

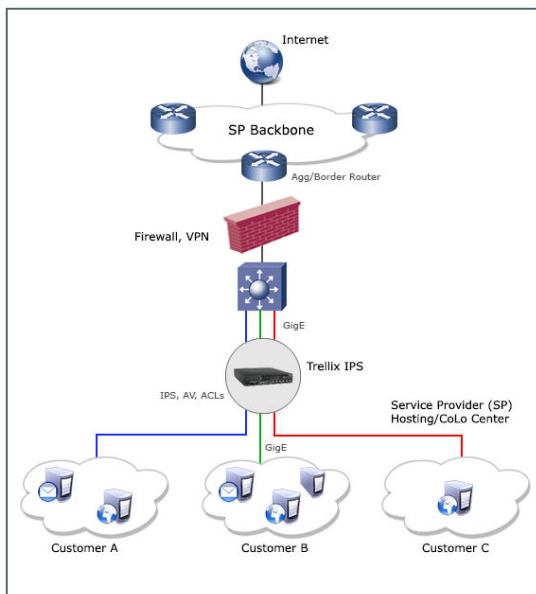
## Deployment of an NS-series Sensor



Deployment of an IPS Sensor requires knowledge of your network to help determine the level of configuration and the number of installed Sensors. You also need to determine the number of Trellix ePolicy Orchestrator - On-prem servers required to protect your network. The Sensor is purpose-built for the monitoring of traffic across one or more network segments.

Following is an example of a network topology using Gigabit Ethernet throughput. In the illustration, Trellix Intrusion Prevention System provides IPS protection to outsourced servers. High port-density and virtualization provides a highly scalable solution, while Trellix IPS protects against web and eCommerce mail server exploits.

#### A sample NS-Series Sensor deployment



:

## NS-series physical description

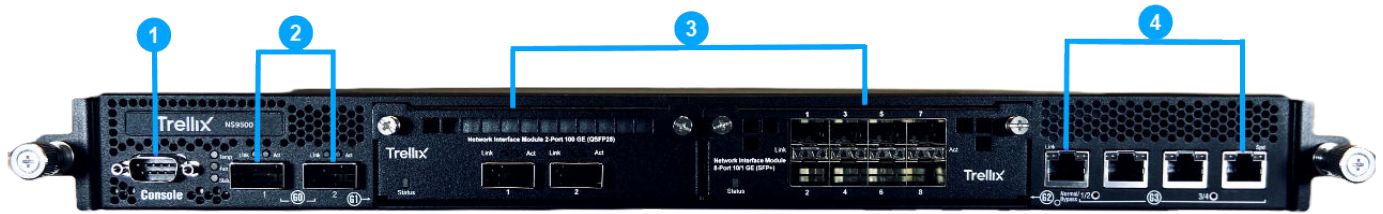
The high-port density NS-series Sensor is designed for high bandwidth links. This section gives a physical description of the NS-series Sensor.

:

### Components of an NS-series Sensor

Correlate the pictures with the information following it to understand the components of an NS-series Sensor.

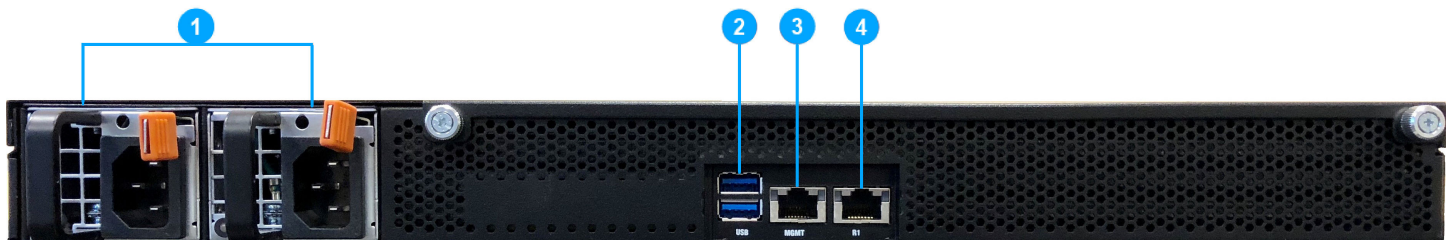
Sensor front panel



1. Console port (1)
2. QSFP28 100/QSFP+ 40 Gigabit Ethernet ports (2)
3. Two slots for I/O modules (Any combination of the interface modules can be used)
  - QSFP28 100/QSFP+ 40 Gigabit Ethernet ports (2)
  - QSFP+ 40 Gigabit Ethernet ports (4)
  - QSFP+ 40 Gigabit Ethernet ports (2)
  - SFP/SFP+ 1/10 Gigabit Ethernet Monitoring ports (8)
  - RJ-45 10/100/1000 Mbps Ethernet Monitoring ports (6)
  - RJ-45 100/1000/10000 Mbps Ethernet Monitoring ports (4)
  - 1/10 Gigabit Ethernet Monitoring ports (4)
  - 100/40 Gigabit SR MTP/MPO passive fail-open (2)
4. RJ-45 100/1000/10000 Mbps Ethernet Monitoring ports (4)

The supported transceiver modules are QSFP28 (MM, SM, and DAC), QSFP+ (MM, SM, and DAC), SFP+ (MM and SM), SFP Fiber (MM and SM) and SFP Copper.

#### 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)

#### Sensor LEDs

:

The front and rear panel LEDs provide status information for the health of the Sensor and the activity on its ports. The following table describes the NS-series LEDs.

### Front panel LEDs

LED	Status	Description
Status	Green Amber	Sensor is operating in good health. Sensor is booting up. It also indicates system bad health if the LED is on for longer duration.
Fan	Green Amber	All five fans are operating. One or more fans are not working.
Temp	Green Amber	Inlet air temperature measured inside the chassis is normal. (Chassis temperature OK) Inlet air temperature measured inside the chassis is too high. (Chassis temperature too hot)
Gigabit Ports Speed	Green Amber Off	The port speed is 10000 Mbps. The port speed is 1000 Mbps. The port speed is 100 Mbps.
Gigabit Ports Link	Green Off	The link is up. The link is down.
RJ45 FailOpen/Bypass	Green Off	The port pair is in Inline Fail-Open/Inline Fail-Close/SPAN/Tap Mode. The Port Pair is in the Bypass Mode.

## Rear panel LEDs

LED	Status	Description
Pwr A (Power A)	Solid Green Blinking Green Solid Amber	Power Supply A is functioning. Power Supply A is stand-by. Power Supply A is not functioning or the unit has no power feed.
Pwr B (Power B)	Solid Green Blinking Green Solid Amber	Power Supply B is functioning. Power Supply B is stand-by. Power Supply B is not functioning or the unit has no power feed.
Management Port Speed	Green Amber Off	The port speed is 10000 Mbps. The port speed is 1000 Mbps.
Management Port Link/Act	Green Blinking Green Off	The link is up. Data is received or transmitted. The link is down.
Response Port Speed	Green Amber Off	The port speed is 10000 Mbps. The port speed is 1000 Mbps.
Response Port Link/Act	Green Blinking Green Off	The link is up. Data is received or transmitted. The link is down.

:

## Before you install

This chapter describes the best practices for deployment of Sensors in your network. Topics include the safety considerations for handling the Sensor, usage restrictions that apply to the Sensor model, and the contents that are shipped along with the Sensor.

:

## Usage restrictions

The following restrictions apply to the use and operation of a Sensor:

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

:

## Safety measures

Please read the following warnings before you install the Sensor. These safety measures apply to all Sensor models unless otherwise noted. Failure to observe these safety warnings could result in serious physical injury.

### Warnings:

- Read the installation instructions before you connect the system to its power source.
- To remove all power from the Sensor, unplug all power cords, including the redundant power cord.
- Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
- Before working on the equipment that is connected to power lines, remove all jewelry including rings, necklaces, and watches. Metal objects will heat up when connected to power and ground, and can cause serious burns or weld the metal object to the terminals.
- This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.
- Do not remove the outer shell of the Sensor. Doing so will invalidate your warranty.
- Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Blank faceplates and cover panels prevent exposure to hazardous voltages and currents inside the chassis, contain electromagnetic interference (EMI) that might disrupt other equipment and direct the flow of cooling air through the chassis.
- To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the users will be required to correct the interference at their own expense.
- Refer to the Appendix for information on regulatory, compliance, and other safety requirements.

:

## About fiber-optic ports

The Sensor uses fiber-optic connectors for its Monitoring ports. The connector and compatible cable types are below:

Connector	Cable
QSFP28	MPO/MTP and LC-duplex
QSFP+	LC-duplex and MPO/MTP
SFP/SFP+	LC-duplex

Note the following:

- Fiber-optic ports (for example, SFP/SFP+/QSFP+/ QSFP28, FDDI, OC-3, OC-12, OC-48, ATM, GBIC, and 100BaseFX) are considered Class 1 laser or Class 1 LED ports.
- These products have been tested and found to comply with Class 1 limits of IEC 60825-1, IEC 60825-2, EN 60825-1, EN 60825-2, and 21CFR1040.

### Caution

To avoid exposure to radiation, do not stare into the aperture of a fiber-optic port. Invisible radiation could be emitted from the aperture of the port when no fiber cable is connected.

- Only FDA registered, EN 60825-1 and IEC 60825-1 certified Class 1 SFP/SFP+/QSFP+/QSFP28 laser transceivers are acceptable for use with the Sensor.

:

## Contents of 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)
- QSFP28 Direct Attach Copper (DAC) cable

:

## Unpack the Sensor

### Steps:

1. Open the crate.
2. Remove the first accessory box.
3. Verify you have received all parts. These parts are listed on the packing list and in *Contents of the box* section.
4. Remove the Sensor.
5. Place the Sensor box as close to the installation site as possible.
6. Position the box with the text upright.
7. Open the top flaps of the box.
8. Remove the accessory box within the Sensor box.
9. Verify you have received all parts. These parts are listed on the packing list and in *Contents of the box* section.
10. Remove the Slide Rail Kit.
11. Pull out the packing material surrounding the Sensor.
12. Remove the Sensor from the antistatic bag.
13. Save the box and packing materials for later use in case you need to move or ship the Sensor.

:

## Setting up the Sensor

This chapter describes how to set up the Sensor for you to configure it.

:

### Setup overview

Setting up a Sensor involves these steps:

1. Position the Sensor.
2. Install the supported interface modules as per your requirement.
3. Attach power, network, and monitoring cables.
4. Turn on the Sensor.
5. Configure the Sensor after you have set up and turned it on.

:

### How to position the Sensor

Place the Sensor in a physically secure location, close to the switches or routers it will be monitoring. Ideally, the Sensor should be located within a standard communications rack. To mount the Sensor on a rack, you will attach two mounting rails to the Sensor as described in the subsequent sections of this guide.

:

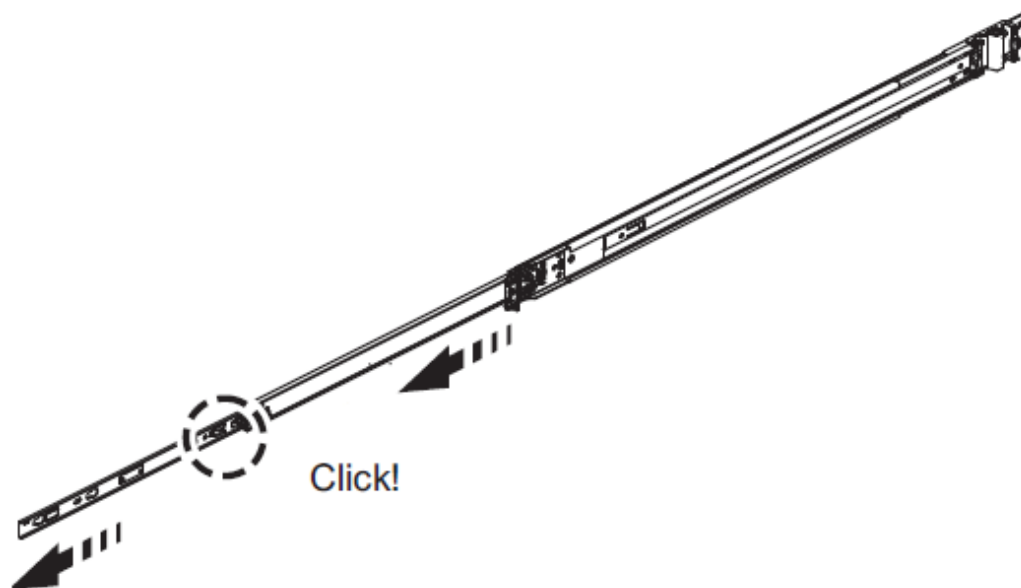
## Install the slide rails and rack mount the Sensor

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

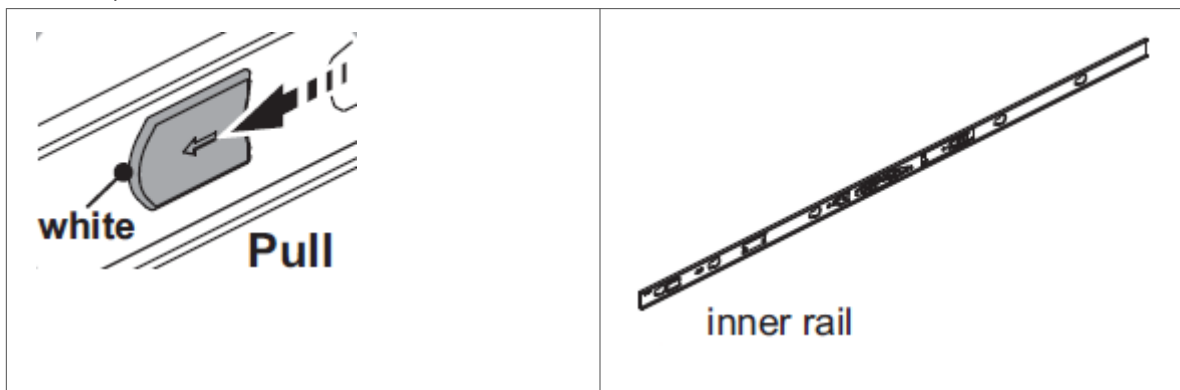
### Note

Due to the weight of the appliance, Trellix recommends that two people place the chassis into the rail cabinet.

1. Disassemble the inner slide rails from the rail assemblies.



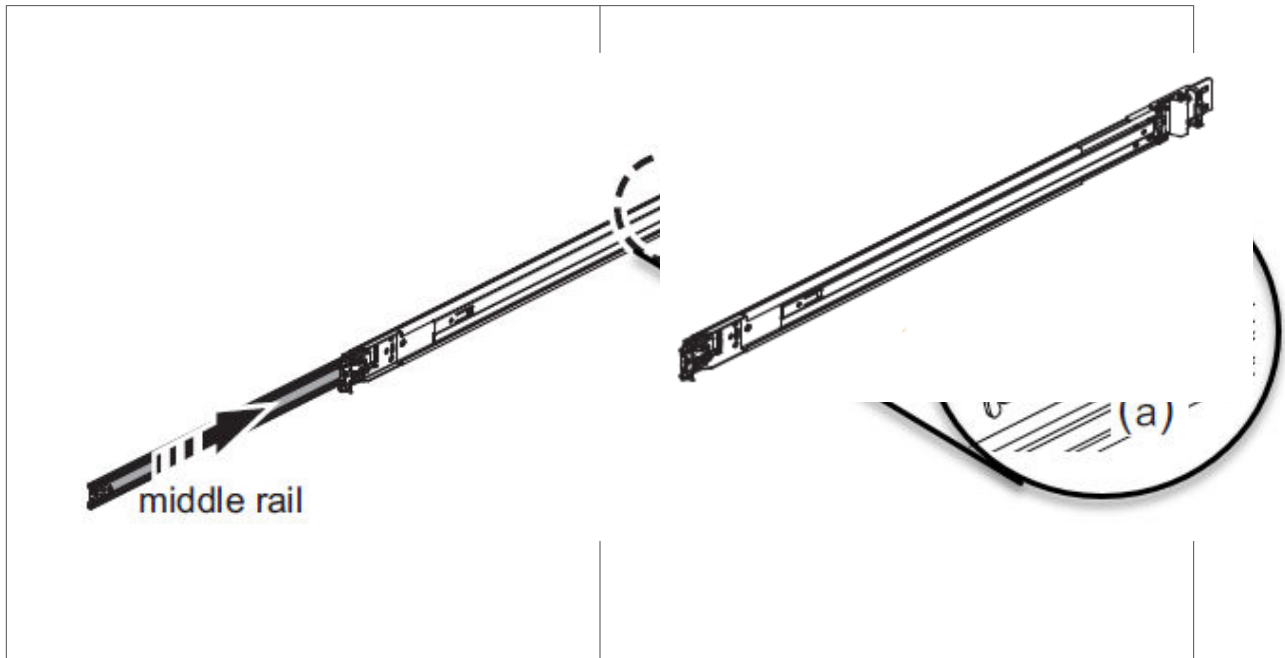
- a. Pull the inner rail out.
- b. Click and pull the white tab (lock on inner rail) forward to disconnect inner rail from the middle rail.





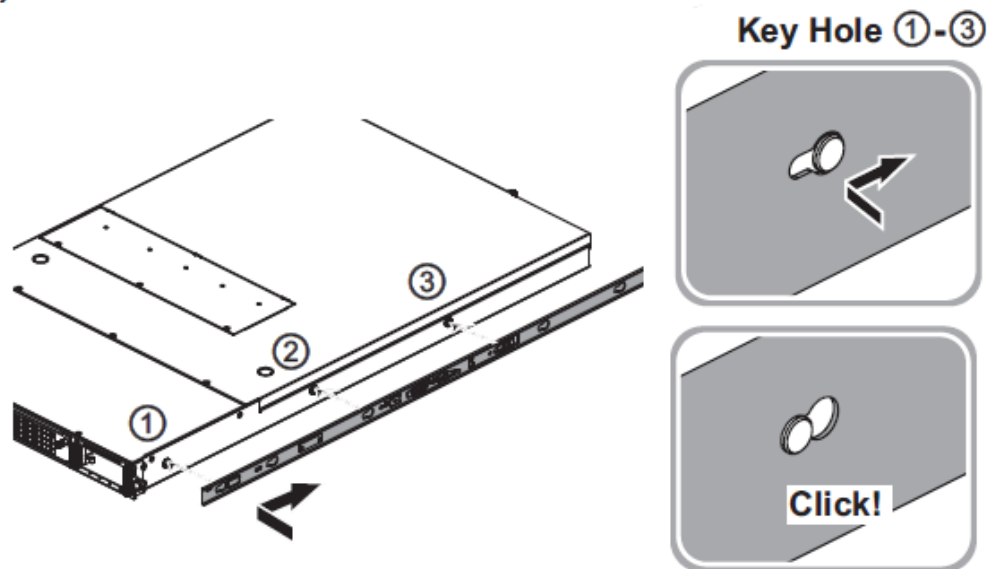
The Inner rail is disconnected.

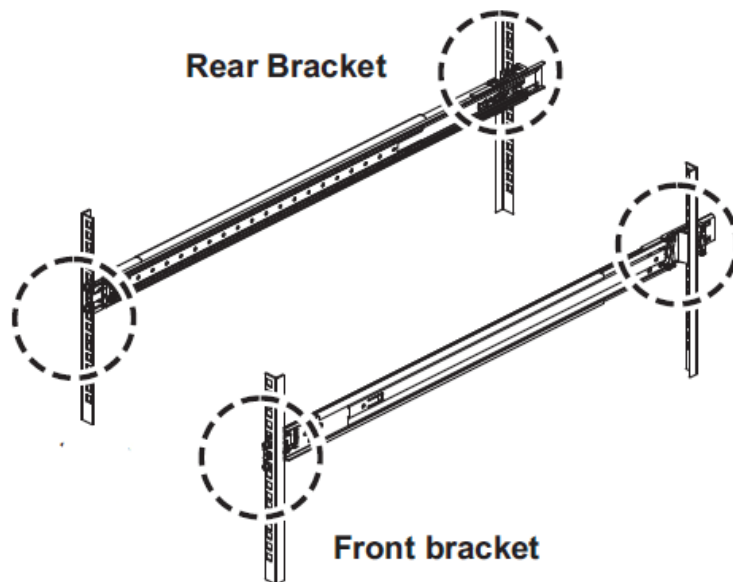
- c. Push tab (a) to slide the middle rail back into the outer rail.



The middle rail is pushed back into the outer rail.

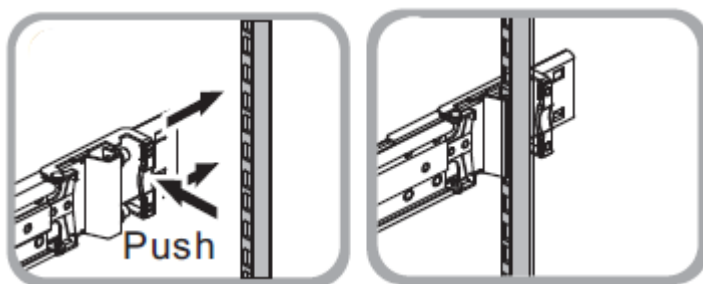
- 2. Mount the inner rail onto the chassis unit.
  - a. Place each inner rail on both sides of the chassis unit. Position the three key holes of the inner rails with the mounting holes on the chassis unit.
  - b. Slide the rails forward to lock it.





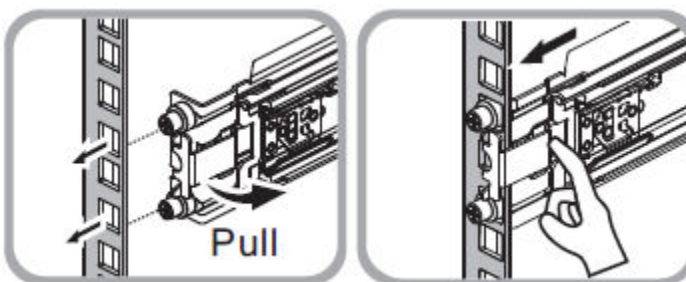
3. Mount the outer slide rails/brackets to the rack posts.

- 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



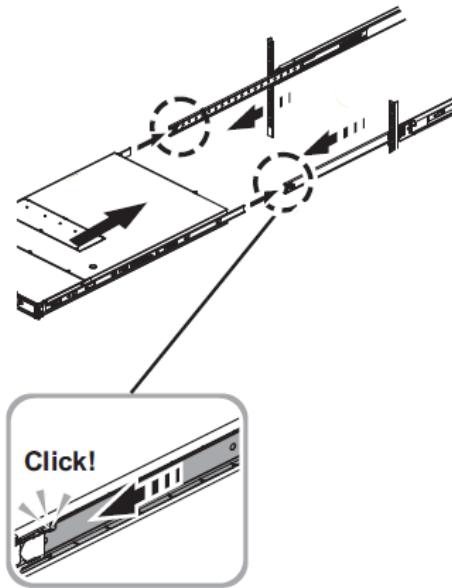
the securing latch onto the rack post.

4. Mount the chassis unit into the rack.

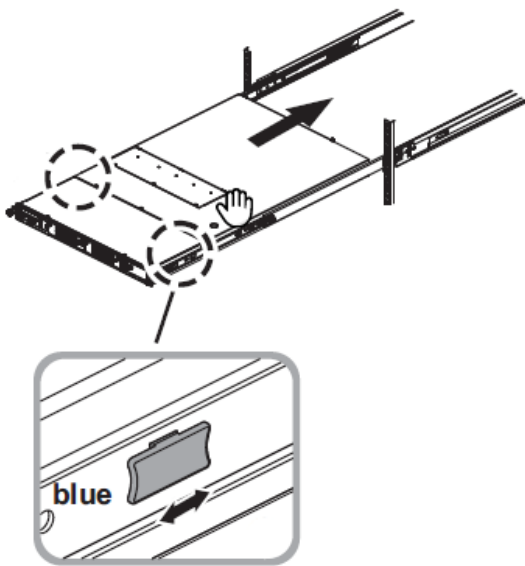
- a. Pull the middle rail out, extend it until the lock position.

 **Note**

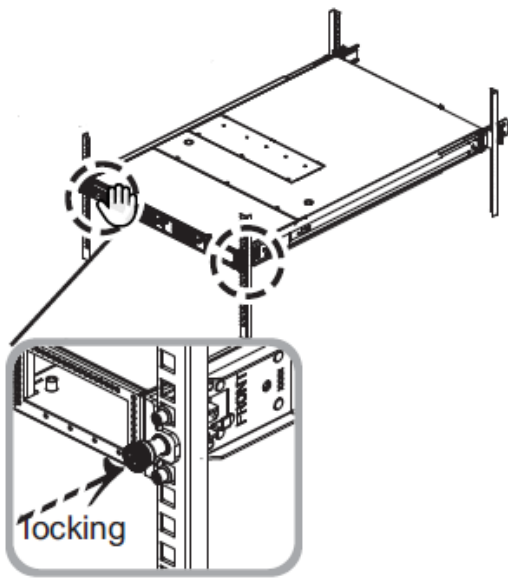
Ensure ball bearing retainer is located at the front of the middle rail.



- 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.



:

## NS-series interface modules

The NS9500 Sensors support the 2-port, 4-port, 6-port, and 8-port Network Interface Modules. These modules need to be installed in the respective slots on the Sensor.

For more information, refer to the *NS-series Interface Modules* section in *Trellix Intrusion Prevention System NS-series Reference Guide*.

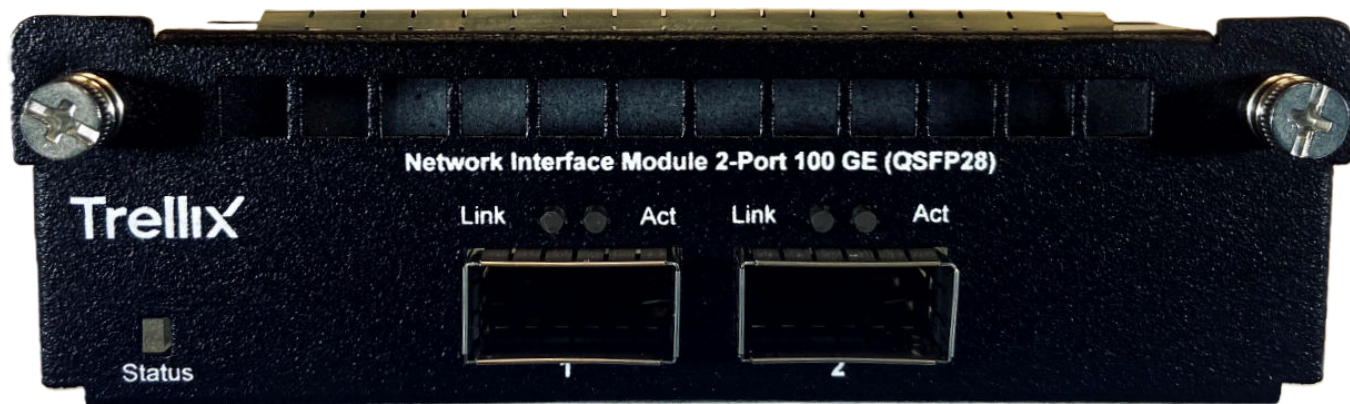
:

### 2-port QSFP28 100 Gigabit Network Interface Module

The 2-port QSFP28 (Quad Small Form-Factor Pluggable 28) Network Interface Module provides 100 Gigabit Ethernet performance on each port.

---

2-port QSFP28 100 Gigabit interface module



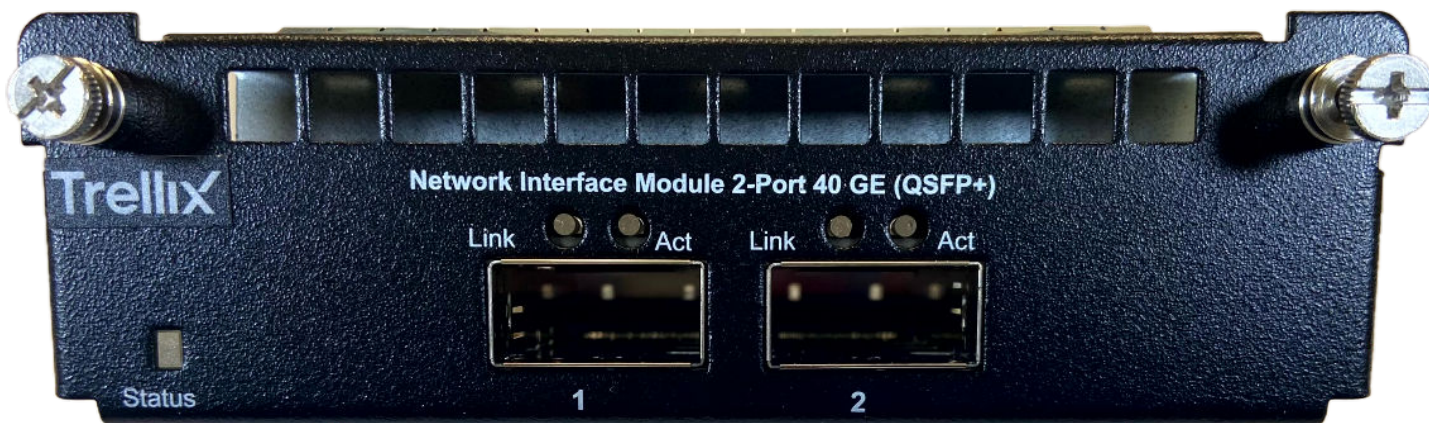
:

### 2-port QSFP+ 40 Gigabit Network Interface Module

The 2-Port QSFP+ (Quad Small Form-Factor Pluggable Plus) Network Interface Module provides 40 Gigabit Ethernet performance on each port.

---

2-Port QSFP+ 40 Gigabit interface module



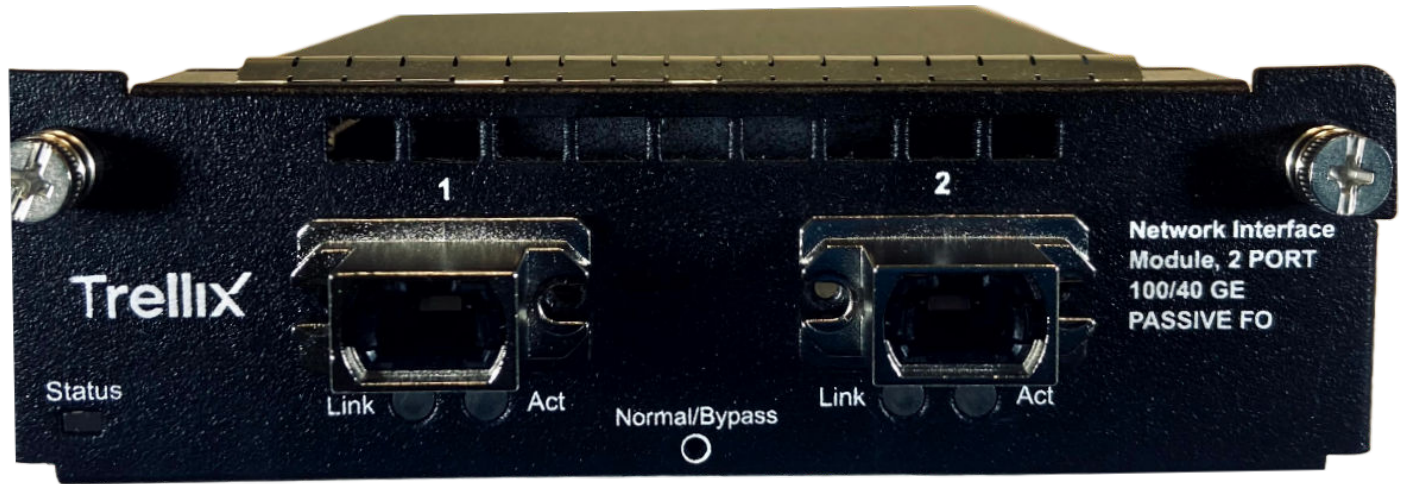
:

### 2-port 100/40 Gigabit SR MTP/MPO passive fail-open interface module

The 2-port 100/40 Gigabit SR MTP/MPO passive fail-open interface module provides internal fail-open capability with 100/40 Gigabit Ethernet performance on each port.

---

2-port 100/40 Gigabit SR MTP/MPO passive fail-open interface module



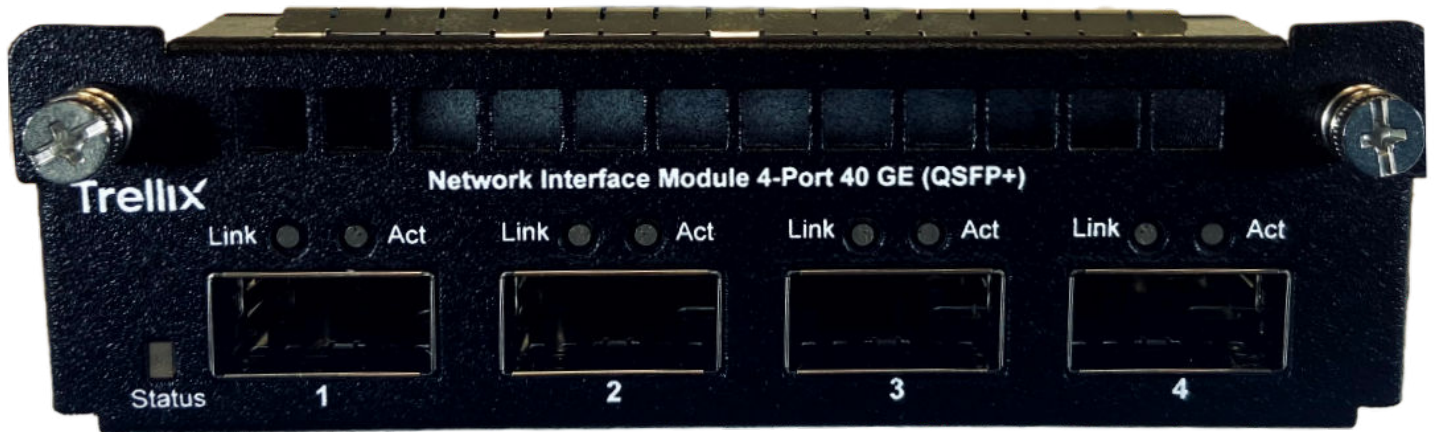
:

### 4-port QSFP+ 40 Gigabit Network Interface Module

The 4-port QSFP+ (Quad Small Form-Factor Pluggable Plus) Network Interface Module provides 40 Gigabit Ethernet performance on each port.

---

4-port QSFP+ 40 Gigabit interface module



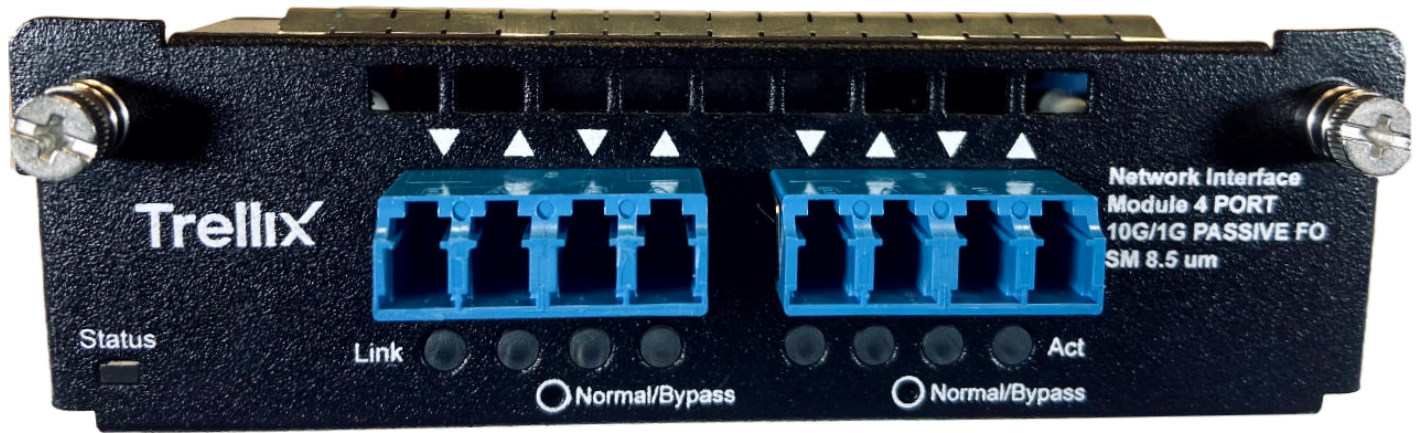
:

### 4-port 10/1 GigE SM 8.5 μm with internal fail-open Network Interface Module

The 4-port SM 8.5 μm Network Interface Module provides internal fail-open capability with 10/1 Gigabit Ethernet performance on each port.

---

4-port 10/1 GigE SM 8.5  $\mu\text{m}$  with internal fail-open interface module

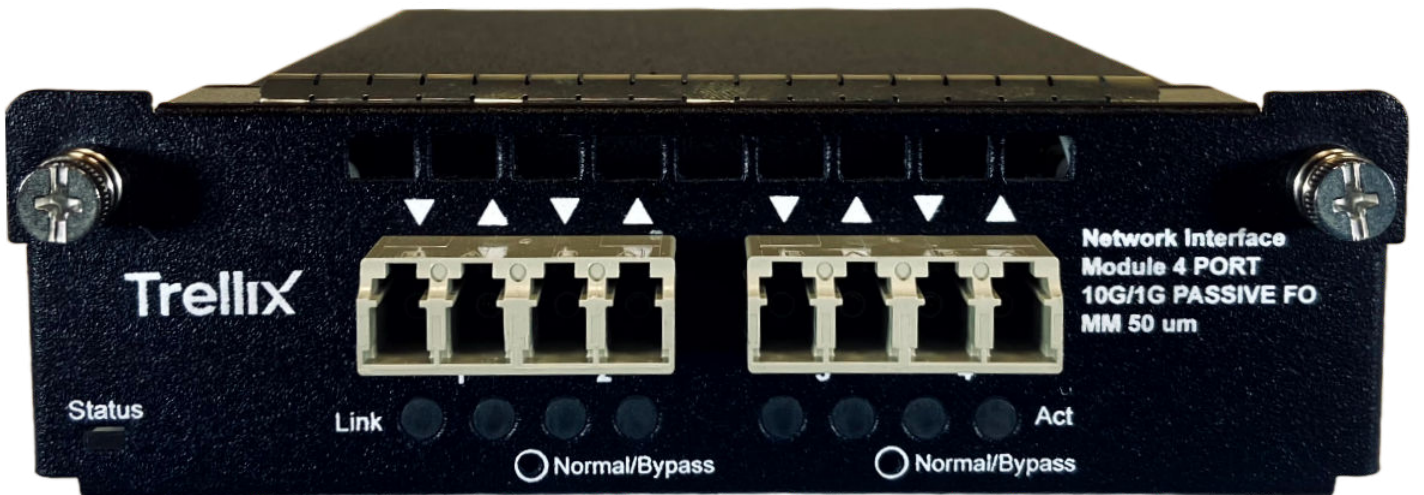


:

### 4-port 10/1 GigE MM 50 $\mu\text{m}$ with internal fail-open Network Interface Module

The 4-port MM 50  $\mu\text{m}$  Network Interface Module provides internal fail-open capability with 10/1 Gigabit Ethernet performance on each port.

4-port 10/1 GigE SM 50  $\mu\text{m}$  with internal fail-open interface module



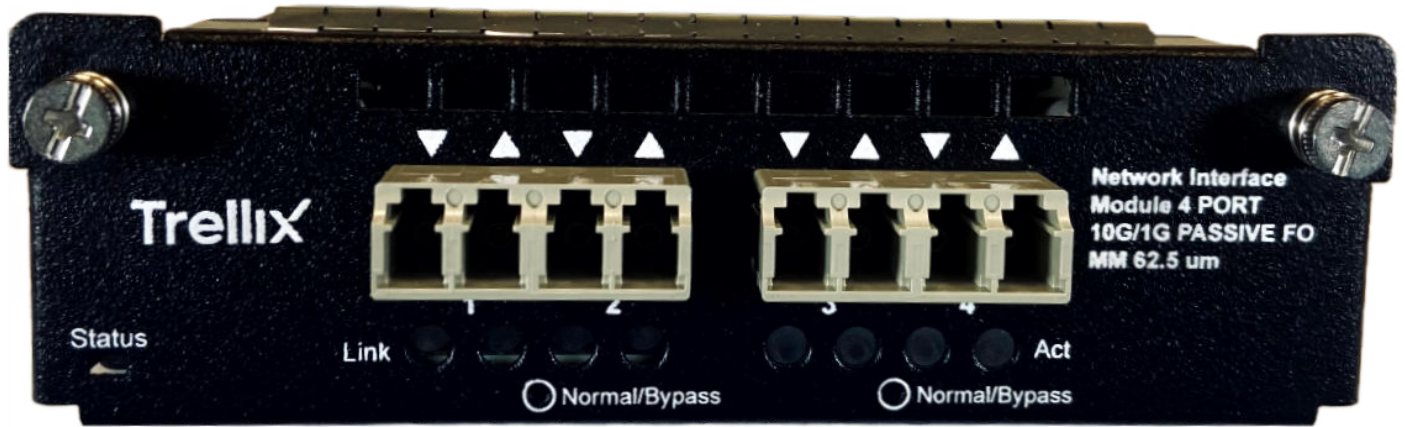
:

### 4-port 10/1 GigE MM 62.5 $\mu\text{m}$ with internal fail-open Network Interface Module

The 4-port MM 62.5  $\mu$ m Network Interface Module provides internal fail-open capability with 10/1 Gigabit Ethernet performance on each port.

---

4-port 10/1 GigE SM 62.5  $\mu$ m with internal fail-open interface module



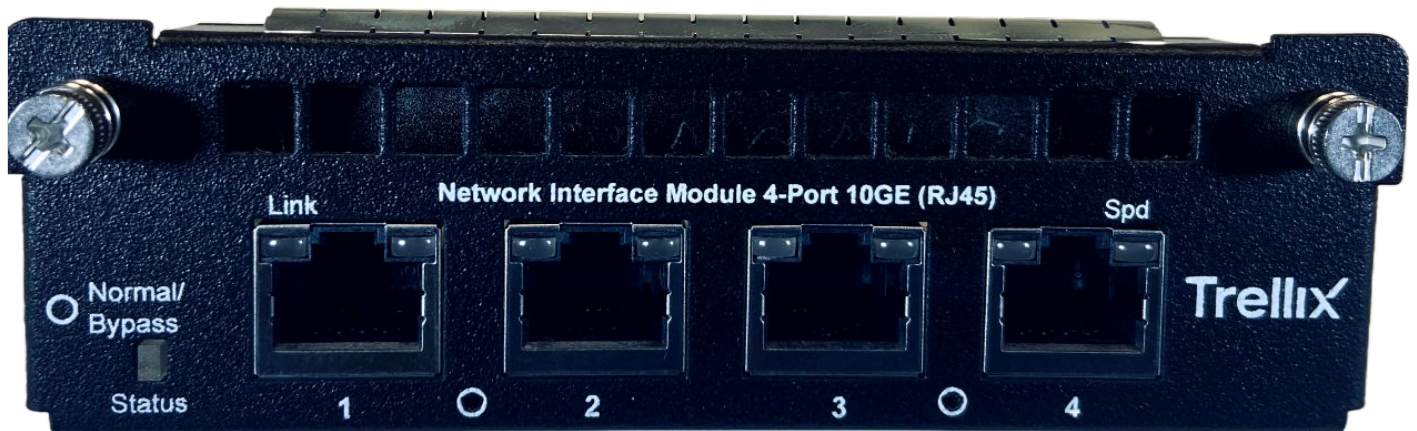
:

### 4-port RJ-45 10 Gbps/1 Gbps/100 Mbps Network Interface Module

The 4-port RJ-45 Network Interface Module provides 10 Gbps/1 Gbps/100 Mbps Ethernet performance on each port.

---

4-port RJ-45 10 Gbps/1 Gbps/100 Mbps interface module



:

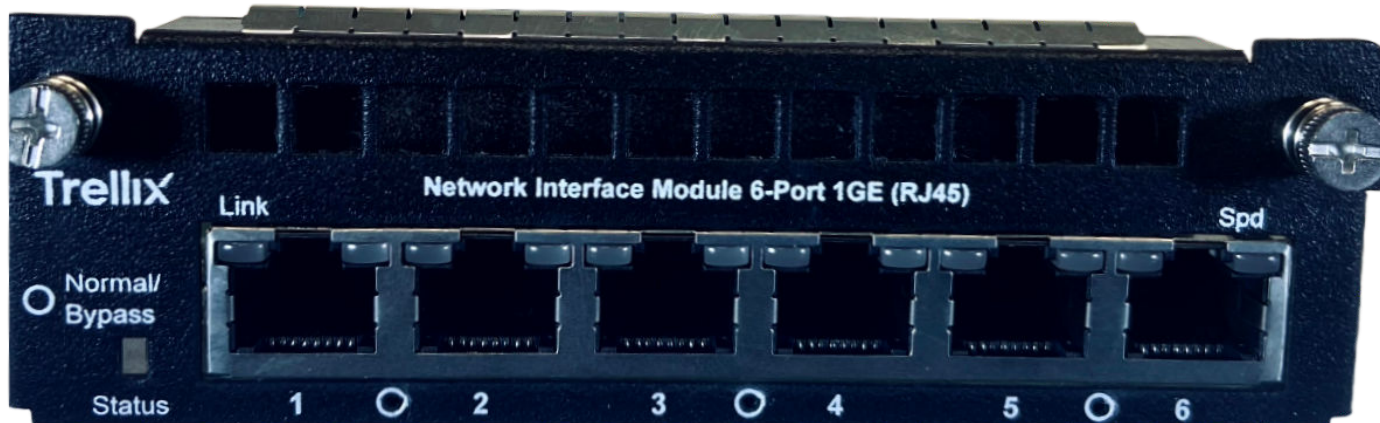


### 6-port RJ-45 10/100/1000 Mbps Network Interface module

The 6-port RJ-45 Network Interface Module provides 10/100/1000 Mbps Ethernet performance on each port.

---

6-port RJ-45 10/100/1000 Mbps interface module



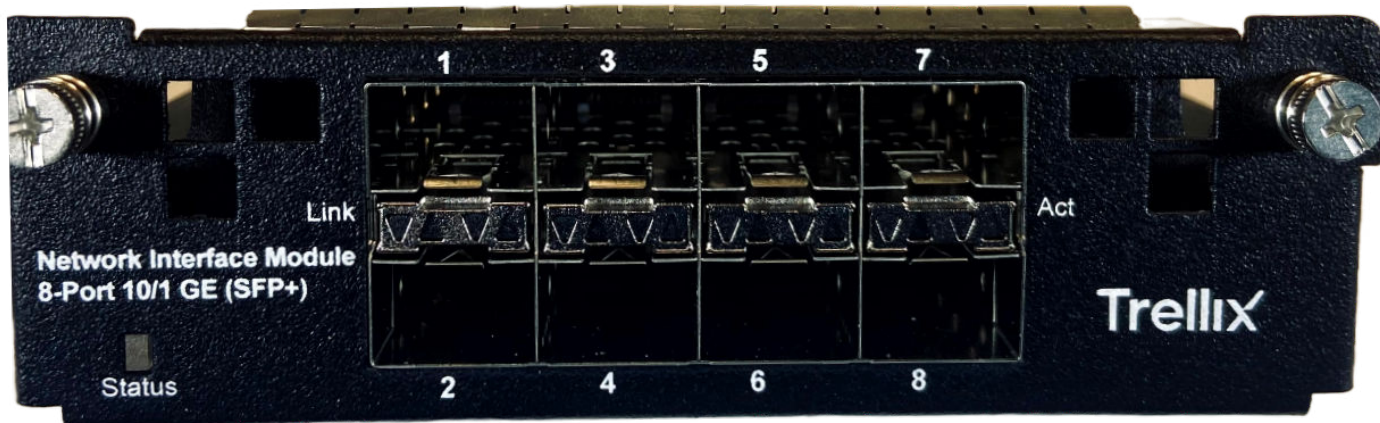
:

### 8-port SFP/SFP+ 1/10 Gigabit Network Interface Module

The 8-Port SFP/SFP+ (Small Form-Factor Pluggable Plus) Network Interface Module provides 1/10 Gigabit Ethernet performance on each port.

---

8-Port SFP+/SFP 10/1G Gigabit interface module



:

## Installation of the interface module

This section provides instructions on how to install the interface module based on the following scenarios:

- Install the interface module during a fresh installation of the Sensor.
- Install the interface module on an up and running Sensor.

:

### Install the interface module during a fresh installation of the Sensor

This section provides the steps to install the interface module for a fresh installation of Trellix Intrusion Prevention System Manager and Sensor.

1. Remove the module from its protective packaging.

#### Note

It is assumed that the Sensor is yet to be powered on, and trust between the Sensor and the Trellix Intrusion Prevention System Manager has not been established.

2. Grip the sides of the module with your thumb and forefinger and insert the module into the slot.

---

#### Install an interface module



3. Drive in the screws fixed on the sides of the module to attach it to the Sensor.
4. Turn on the Sensor.
5. Establish trust between the Sensor and the Trellix IPS Manager.

:

## Install the interface module on an up and running Sensor

This section provides the steps to install the interface module on a Sensor which is up and running.

1. Power on the Sensor without inserting the pluggable module(s) into the slot(s).
2. Establish trust between the Sensor and the IPS Manager.
3. Grip the sides of the module with your thumb and forefinger and insert the module into the slot.
4. Wait for 5 minutes.
5. Reboot the Sensor from the CLI.

:

## Remove an interface module

Perform these steps if you need to remove an interface module.

1. Disconnect the network fiber optic cable from the module.
2. Remove the transceivers from the module.
3. Unscrew the interface modules to detach them from the Sensor.
4. Place the module into its protective packaging.

:

## Small form-factor pluggable transceiver modules

The NS-series Sensors use four types of small form-factor pluggable transceiver modules as shown in the following table. For more information, see the section *NS-series Transceiver Modules* in *Trellix Intrusion Prevention System NS-series Reference Guide*.

Type	Performance
SFP	1 Gbps (copper) 1 Gbps (fiber optic)
SFP+	10 Gbps (fiber optic)
QSFP+	40 Gbps (fiber optic)
QSFP28	100 Gbps (fiber optic)

Each module is an input/output device that plugs into an LC-type Gigabit Ethernet port, linking the module port with a copper or fiber-optic network. SFP optical interfaces are less than half the size of GBIC interfaces.

To ensure compatibility, Trellix supports only those SFP, SFP+, QSFP+ and QSFP28 modules purchased through Trellix or from a Trellix-approved vendor. For a list of approved vendors, locate the relevant KnowledgeBase article at <https://supportm.trellix.com>. Enter the relevant KnowledgeBase article in Search the Support Knowledge Center and click Search to locate the article.

These installation instructions provide information for installing SFP, SFP+, QSFP+ and QSFP28 modules that use a bail clasp for securing the module in place in the Sensor. Your module might be slightly different. Check the module manufacturer's installation instructions for more details. For ease of installation, insert the module in the Sensor while it is turned off and before placing it on a rack.

### Caution

To prevent eye damage, do not stare into open laser apertures.

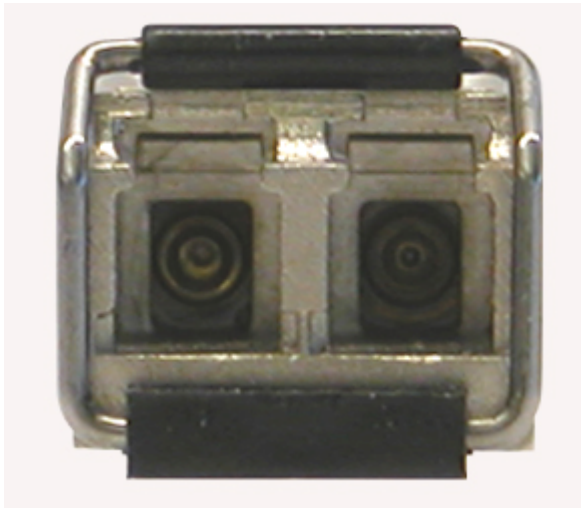
:

## SFP transceiver modules

An SFP module is a protocol-independent, compact, optical receiver, which allows for greater port density than the standard GBIC. This module operates at varying speeds for up to 1 gigabit per second on SONET/SDH, Fibre Channel, Gigabit Ethernet and other applications. An SFP module operates in multimode. Additionally, this module transmits on a 850-nanometer wavelength on short reach (SR) and 1310-nanometer long reach (LR).

---

An SFP module



:

## SFP+ transceiver modules

The enhanced small form-factor pluggable ( SFP+ ) is an enhanced version of the SFP that supports data rates up to 10 Gbps. 850nm SFP+ 1310nm SFP+Transceiver modules are supported.

850nm SFP+ transceiver module



1310nm SFP+ transceiver module



:

### QSFP+ transceiver modules

The Quad Small Form-factor Pluggable (QSFP+) is a compact, hot-pluggable, protocol-independent transceiver used for data communications applications. It interfaces a network device (switch, router, media converter or similar device) to a fiber optic cable. It is a industry format jointly developed and supported by many network component vendors. QSFP+ transceivers are designed to support Serial Attached SCSI, 40G Ethernet, 20G/40G Infiniband, and other communications standards. 850nm (short reach - SR) and 1310 nm (long reach - LR) QSFP+ transceiver modules are supported.

---

850nm QSFP+ transceiver module



:

### QSFP28 transceiver modules

The Quad Small Form-factor Pluggable (QSFP28) is a compact, hot-pluggable, transceiver used for data communications applications. It interfaces a network device (switch, router, media converter or similar device) to a fiber optic cable. It is an industry format jointly developed and supported by many network component vendors. QSFP28 transceivers are specifically designed to support 100G Ethernet. This module transmits on long reach (LR), short reach (SR), and Copper (CU).

---

### 850nm QSFP28 transceiver module



:

## Install a transceiver module

1. Remove the module from its protective packaging.
2. Locate the label on the module and make sure that the alignment groove is down.
3. Grip the sides of the module with your thumb and forefinger and insert the module into the module socket. Modules are keyed to prevent incorrect insertion.

---

Insert a transceiver module



### Important

In the following scenarios, you need to reboot the Sensor to detect the new speed:

- 100 Gbps DAC to 40 Gbps DAC or vice versa
- 100 Gbps Fiber transceiver to 40 Gbps Fiber transceiver or vice versa

:

## Remove a transceiver module

Perform these tasks if you need to remove a module.

**Steps:**

1. Disconnect the network fiber-optic cable from the module.
2. Release the module from the slot by pulling the bail clasp out of its locked position.
3. Slide the module out of the slot.
4. Insert the module plug into the module optical bore for protection.

:

## Attaching cables to the Sensor

Follow the steps outlined in this chapter to connect the cables to the various ports of your Sensor.

:

### Connect the cable to the Console port

The Console port on the NS-series Sensor is used for setup and configuration of the Sensor.

**Steps:**

1. For console connections, plug the DB9 Console cable supplied by Trellix into the Console port on the Sensor. This port is labeled **Console** in the Sensor front panel.
2. Connect the other end of the Console port cable directly to a COM port of the computer or terminal server you will use to configure the Sensor, for example, a computer 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. Required settings for HyperTerminal are listed below:

Name	Setting
Baud rate	115200
Number of bits	8
Parity	None
Stop bits	1
Flow control	None

3. Turn on the Sensor.



:

## Connect the cable to the Response port

When operating in tap or SPAN mode, the Sensor uses its Response port to respond to attacks. When deployed in tap mode, the Sensor does not inject response packets through the tap but uses the Response port.

### Steps:

1. Plug a Cat-5e Ethernet cable into the Response port. This port is labeled **R1** on the Sensor rear panel.
2. Connect the other end of the cable to the network device, such as a hub, switch, or a router, through which you want to respond to attacks.

:

## Connect the cable to the Management port

The Sensor communicates with the Manager using the Management port.

1. Plug a Category 5e Ethernet cable into the Management port. This port is labeled **Mgmt** in the rear panel of the NS-series Sensor.
2. Plug the other end of the cable into the network device connected to your Manager server.

### Note

To isolate and protect your management traffic, Trellix strongly recommends you to use a separate, dedicated management subnet to interconnect the Sensors and the Manager.

:

## About connecting cables to the Monitoring ports

Connect to the network devices that you want to monitor through the Sensor monitoring ports. You can deploy Sensors in the following operating modes:

- In-line mode (fail-close)
- In-line mode (fail-open)
- External tap mode
- SPAN or hub mode

:

## How to use peer ports

You must use two peer Monitoring ports of the Sensor to deploy it full duplex mode. On the Sensor, the numbered ports are wired in pairs to accommodate the traffic.

The following Ethernet ports are coupled and must be used together.

#### Note

- On NS9500 Sensors, G0 and G3 indicate the fixed port slots. G1 and G2 indicate the slots for interface modules.
- In the following table, it is assumed that G1 is the 2-port QSFP28 1000G interface module, G2 is the 8-Port SFP+/SFP 1/10G interface module, G5 is the 4-port QSFP+ 40G interface module and G6 is the 6-port RJ-45 1 Gbps/100 Mbps/10 Mbps interface module. These interface modules can be interchanged.
- Since monitoring ports are internally wired, when you disable one of the ports in a pair, the corresponding port is also disabled.

#### Note

You cannot disable auto-negotiation in G3 slots.

Port Pairs	Sensor	Interface module
G0/1 and G0/2	NS9500	2-port QSFP28 100 Gigabit Network Interface Module
G1/1 and G1/2	NS9500	
G2/1 and G2/2	NS9500	8-port SFP/SFP+ 1/10 Gigabit Network Interface Module
G2/3 and G2/4	NS9500	
G2/5 and G2/6	NS9500	
G2/7 and G2/8	NS9500	
G3/1 and G3/2	NS9500	4-port QSFP+ 40 Gigabit Network Interface Module
G3/3 and G3/4	NS9500	6-port RJ-45 10/100/1000 Mbps Network Interface module

:

## Cable types for routers, switches, hubs, and computers

This section lists the types of cables that you require to connect the Sensor to other network devices:

- Use a crossover Ethernet RJ-45 cable to connect a router port to computer to the Sensor Management port.
- Use a crossover Ethernet RJ-45 cable to connect a computer to the Sensor monitoring port.

:

## Connect the cables for in-line mode

In-line Gigabit Ethernet ports can be configured as fail-open or fail-closed. The RJ-45 monitoring ports are built-in and include an built-in fail-open functionality as well.

All other monitoring ports require the use of either Trellix's 4-port 1/10 Gigabit Modular Passive Fail-Open kit or external active fail-open (AFO) kits for In-Line Fail-Open Active configuration.

Gigabit Ethernet ports fail-close, means the flow of traffic will stop if the Sensor fails. To allow traffic to flow uninterrupted, you must use special hardware, and cable the Sensor to external active fail-open kits. For instructions, see the subsequent sections of this chapter.

This section provides the steps to connect the Sensor's Gigabit Ethernet ports so they fail-close.

1. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports, for example G1/1.
2. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports, for example G1/2.
3. 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 switch and the one connected to 2 to the router.

:

## Connect the cables for tap mode

To deploy the Sensor in tap mode, you must use a Sensor's Gigabit Ethernet Monitoring port pair with a third-party external tap.

### Note

For a list of Trellix-approved third party vendors, see the KnowledgeBase at <https://supportm.trellix.com>. Enter the relevant KnowledgeBase article in Search the Support Knowledge Center and click Search to locate the relevant KnowledgeBase article.

**Steps:**

1. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports, for example, G1/1.
2. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports labeled G1/2.
3. Connect the other end of each cable to the tap.
4. Connect the network devices that you want to monitor to the tap.

:

## Connect the cables for SPAN or hub mode

For the Sensor, monitoring in SPAN or hub mode occurs in in-line fail-open mode. When you monitor in SPAN or hub mode, you use only single ports.

To connect an Sensor to a SPAN port or hub, plug an LC fiber-optic or 45 cable into one of the modules and connect the other end of the cable to the SPAN port or the hub.

:

## Connect the cable for standalone Sensor failover

For Sensor failover, connect two NS-series Sensors using the appropriate cables. These two Sensors must be running the same software version. Failover cables are the only additional hardware required to support failover communication between two NS-series Sensors.

Refer the following table before you configure a HA pair:

Sensor Model	Port to connect the HA pair	Cable requirements for failover
NS9500	G0/1	QSFP28/QSFP+ Direct Attach Copper (DAC)

You can use 2-port QSFP28 interface module, or 2-port QSFP+ interface module or 4-port QSFP+ interface module for Sensor failover. Port G1/1 is used for failover. G1/2 is unusable. For 4-port interface module, ports G1/3 and G1/4 can be used as monitoring ports.

The system ships with a 1m QSFP28 DAC cable. This can be used for failover connection if the failover sensors are placed within 1m.

If you need to configure HA pair between sensors kept at distance greater than 1m, consider the following options:

- For distances up to 3m, purchase QSFP28 DAC from Trellix.
- For distances greater than 3m, purchase 40G QSFP transceivers from Trellix and fiber cables from external vendor.

1. Plug the cable(s) appropriate for use with your QSFP+ or QSFP28 module into port G0/1 (NS9500) of the active NS-series Sensor.
2. Connect the other end of the cable(s) into port G0/1 (NS9500) of the standby NS-series Sensor.

:

### Connect the cables for Sensor Fail-Open

The Fail-Open Kits minimize the potential risks of in-line Sensor failure on critical network links. You need to purchase these kits separately. Both copper and optical versions of the kit are available for the one-gigabit ports. The standard Gigabit Fail-Open Kits, 10 Gigabit Fail-Open Kits and 40 Gigabit Fail-open Kits are available for the 1, 10, and 40 gigabit ports respectively.

The Monitoring ports of the Sensors can be fail-close; thus, if the Sensor is deployed in-line fail-close, a hardware failure results in network downtime. Except the built-in RJ-45 ports which come with built-in fail-open functionality, you use either the optional Trellix's 4-port 1/10 Gigabit Modular Passive Fail-Open kit or external bypass switch provided in an Active Fail-Open Kit for the Monitoring ports to fail-open.

While the Sensor is operating, the Active Fail-Open kit is in-line and routes all traffic directly through the Sensor. When the Sensor fails, the switch automatically shifts to a bypass state; in-line traffic continues to flow through the network link but is no longer routed through the Sensor. After the Sensor resumes normal operation, the switch returns to the "on" state, enabling in-line monitoring once again.

#### Caution

Sensor outage breaks the link connecting the devices on either side of the Sensor for a brief moment and requires the renegotiation of the network link between the two peer devices connected to the Sensor. Depending on the network equipment, this disruption introduced by the renegotiation of the link layer between the two peer devices might range from a couple of seconds to more than a minute with certain vendors' devices.

#### Caution

A very brief link disruption might also occur while the links between the Sensor and each of the peer devices are renegotiated to place the Sensor back in in-line mode. This outage, again, varies depending on the device, and can range from a few seconds to more than a minute.

The performance of the switchover from in-line to bypass and vice versa varies depending on the vendor.

You can find the installation and troubleshooting instructions for the kit in the guide that accompanies the kit. For example, for more information on the Optical kits, see the following guides:

- *1 Gigabit Optical Active Fail-Open Bypass Kit Guide*
- *10 Gigabit Optical Active Fail-Open Bypass Kit Guide*
- *40 Gigabit Optical Active Fail-Open Bypass Kit Guide*

- *Active Fail-Open Kit Quick Start Guide*
- *Passive Fail-Open Kit Quick Start Guide*

:

### Turning the Sensor on and off

#### Note

Do not attempt to turn on the Sensor until you have installed the Sensor in a rack and made all the necessary network connections.

#### Steps:

1. Connect the power cable to the Sensor power supply.
2. Connect the power cable to a power source.

#### Note

If you are installing a redundant power supply, you should install it as described in *Install a new power supply* section. For true redundant operation with the optional redundant power supply, Trellix recommends that you plug each supply into a different power circuit.

The Sensor has no power switch. The Sensor turns on as soon as one of its power cables is connected to a power source. Trellix recommends that you use the **shutdown** CLI command to halt the Sensor before turning it off. For more information on CLI commands, see the *CLI commands* section in *Trellix Intrusion Prevention System Product Guide* for specific Sensor software version you are running.

:

### License requirement for NS9500 Sensors

The NS9500 Sensor requires a license to activate the baseline throughput. You must first purchase a license to enable traffic inspection in the NS9500 Sensor. To obtain a license, contact **Trellix Sales**. Additional license is required to increase the throughput of the Sensor.

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 capacity licenses available for the NS9500 Sensors:

License SKUs	Throughput	Number of Sensors
NS95X10CAE-AT	10 Gbps	1 NS9500 Sensor
NS95X20CAE-AT	20 Gbps	1 NS9500 Sensor
NS95X30CAE-AT	30 Gbps	1 NS9500 Sensor
NS95X40CAE-AT	40 Gbps	Stack of 2 NS9500 Sensors
NS95X60CAE-AT	60 Gbps	Stack of 2 NS9500 Sensors
NS95X100CAE-AT	100 Gbps	Stack of 4 NS9500 Sensors

The table below shows the upgrade capacity licenses available for the NS9500 Sensors:

License SKUs	Throughput	Number of Sensors
NS95X1020CAE-DT	10 to 20 Gbps	1 NS9500 Sensor
NS95X1030CAE-DT	10 to 30 Gbps	1 NS9500 Sensor
NS95X1040CAE-DT	10 to 40 Gbps	2 NS9500 Sensor
NS95X1060CAE-DT	10 to 60 Gbps	2 NS9500 Sensors
NS95X10100CAE-DT	10 to 100 Gbps	4 NS9500 Sensors
NS95X2030CAE-DT	20 to 30 Gbps	1 NS9500 Sensor
NS95X2040CAE-DT	20 to 40 Gbps	2 NS9500 Sensor
NS95X2060CAE-DT	20 to 60 Gbps	2 NS9500 Sensors
NS95X20100CAE-DT	20 to 100 Gbps	4 NS9500 Sensors

License SKUs	Throughput	Number of Sensors
NS95X3040CAE-DT	30 to 40 Gbps	2 NS9500 Sensor
NS95X3060CAE-DT	30 to 60 Gbps	2 NS9500 Sensors
NS95X30100CAE-DT	30 to 100 Gbps	4 NS9500 Sensors
NS95X4060CAE-DT	40 to 60 Gbps	2 NS9500 Sensors
NS95X40100CAE-DT	40 to 100 Gbps	4 NS9500 Sensors
NS95X60100CAE-DT	60 to 100 Gbps	4 NS9500 Sensors

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 licenses, see [Managing licenses for NS9500 Sensors](#).

:

## License requirement for NS9500 Sensor failover

Based on the throughput, the NS9500 Sensor requires an additional license for Sensor failover. 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 capacity licenses available for the NS9500 Sensor failover:

License SKUs	Throughput	Number of Sensors
FO95X10CAE-AT	10 Gbps	2 * 1 NS9500 Sensor
FO95X20CAE-AT	20 Gbps	2 * 1 NS9500 Sensor
FO95X30CAE-AT	30 Gbps	2 * 1 NS9500 Sensor



License SKUs	Throughput	Number of Sensors
FO95X40CAE-AT	40 Gbps	2 * 2 NS9500 Sensors
FO95X60CAE-AT	60 Gbps	2 * 2 NS9500 Sensors
FO95X100CAE-AT	100 Gbps	2 * 4 NS9500 Sensors

The table below shows the upgrade capacity licenses available for the NS9500 Sensor failover:

License SKUs	Throughput	Number of Sensors
NS95XF1020CAE-DT	10 to 20 Gbps	2 * 1 NS9500 Sensor
NS95XF1030CAE-DT	10 to 30 Gbps	2 * 1 NS9500 Sensor
NS95XF1040CAE-DT	10 to 40 Gbps	2 * 2 NS9500 Sensor
NS95XF1060CAE-DT	10 to 60 Gbps	2 * 2 NS9500 Sensors
NS95XF10100CAE-DT	10 to 100 Gbps	2 * 4 NS9500 Sensors
NS95XF2030CAE-DT	20 to 30 Gbps	2 * 1 NS9500 Sensor
NS95XF2040CAE-DT	20 to 40 Gbps	2 * 2 NS9500 Sensor
NS95XF2060CAE-DT	20 to 60 Gbps	2 * 2 NS9500 Sensors
NS95XF20100CAE-DT	20 to 100 Gbps	2 * 4 NS9500 Sensors
NS95XF3040CAE-DT	30 to 40 Gbps	2 * 2 NS9500 Sensor
NS95XF3060CAE-DT	30 to 60 Gbps	2 * 2 NS9500 Sensors
NS95XF30100CAE-DT	30 to 100 Gbps	2 * 4 NS9500 Sensors

License SKUs	Throughput	Number of Sensors
NS95XF4060CAE-DT	40 to 60 Gbps	2 * 2 NS9500 Sensors
NS95XF40100CAE-DT	40 to 100 Gbps	2 * 4 NS9500 Sensors
NS95XF60100CAE-DT	60 to 100 Gbps	2 * 4 NS9500 Sensors

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

:

## Managing licenses for NS9500 Sensors

The NS9500 Sensor requires a license to activate the baseline throughput of 10 Gbps. Additional license is required to increase the throughput from 10 Gbps to 20 Gbps or 30 Gbps. The license is provided as a .zip or .jar file. The Manager supports both formats. The license procured contains the details for the throughput for the Sensors.

### Note

You must first purchase a license to enable traffic inspection in the NS9500 Sensor. To obtain a license, contact the Sales team.

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

The following details are displayed in the Capacity tab:

---

Upload license capacity for Sensor

/My Company > Setup > Licenses




### Licenses



System | Proxy Decryption | Virtual Sensors

Quick Search Clear All Filters

	Required		Assigned To	License Details				Added
	Model	Capacity ↓		Customer	Grant ID	Key	Expiration	Time
1	IPS-NS9500	10 Gbps	---	---	---	---	---	Oct 15 2020 10:08:32
2	IPS-NS9500	10 Gbps	---	---	---	---	---	Oct 15 2020 10:08:32
3	IPS-NS7500	3 Gbps	---	---	---	---	---	Oct 15 2020 10:06:29

+ - | Assign Unassign | Save as CSV 3 licenses

Option	Definition
Required	Model – Sensor model compatible with the license Capacity – Throughput limit for the license Device Count – Number of devices that can be assigned to the license
Assigned To	Name of the Sensor assigned to the license.
License Details	Customer – Customer for whom the license file was generated Grant ID – The Trellix Grant ID of the corresponding customer Key – The license key number. Expiration – Applicable only for demo and subscription licenses <ul style="list-style-type: none"> <li>•  : Valid license</li> <li>•  : Expired license</li> <li>•  : Expired license running on grace period</li> </ul>

Option	Definition
	<p> <b>Note:</b> A grace period of <b>30 days</b> is provided to subscription-based System licenses after they expire.</p> <p>Post grace period, the Sensor continues to inspect traffic, and operates with the existing signature set and configuration. The Manager, however, will not be able to deploy new signature sets or policies to the Sensor until a valid license is assigned.</p> <p>Type – Displays if the license is Perpetual, Subscription, or Evaluation (Demo) type.</p> <p> <b>Note:</b> It is recommended to install subscription license from Manager version 10.1.7.44 and later.</p>
Added	<p>Time – Date in &lt;mmm-yy&gt; format, and time when the license was added</p> <p>By – Name of the user who added the license</p>
Comments	<p>Enables you to add your comment per license file that is imported. Double-click in the Comment field and enter your comment. Click outside this field and your comment is automatically saved.</p>


The following actions can be performed in the Capacity tab:

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

:

## [Add license to the Manager](#)

To upload the license, perform the following steps:

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

 **Note**

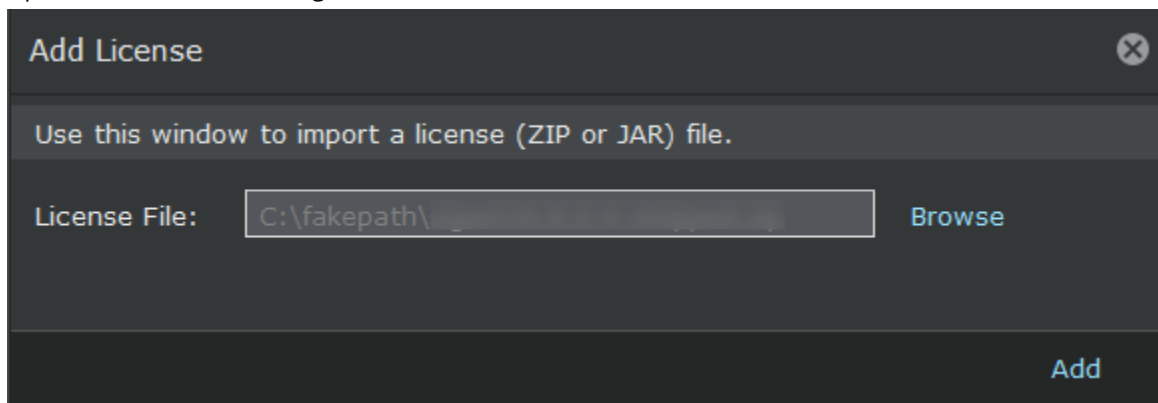
The supported license formats are zip and jar.

 **Note**

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

---

Upload license to the Manager



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

:

### Assign a license to a Sensor

To assign the license, perform the following steps:

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

/My Company > Setup > Licenses

Licenses

System Proxy Decryption Virtual Sensors

Quick Search Clear All Filters

	Required		Assigned To	License Details				Type
	Model	Capacity ↓		Customer	Grant ID	Key	Expiration	
1	IPS-NS9500	100 Gbps	---					Subscription
2	IPS-NS9500	100 Gbps	---					Subscription
3	IPS-NS9500	100 Gbps	---					Subscription
4	IPS-NS9500	100 Gbps	---					Subscription
5	IPS-NS9500	100 Gbps	---					Subscription
6	IPS-NS9500	100 Gbps	---					Subscription
7	IPS-NS9500	100 Gbps	---					Subscription

+ - Assign Unassign Save as CSV 55 licenses

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

Assign License

Model: IPS-NS9500

Capacity: 30 Gbps

Grant ID: [Redacted]

Key: [Redacted]

Expiration:  Dec 31 [Redacted]

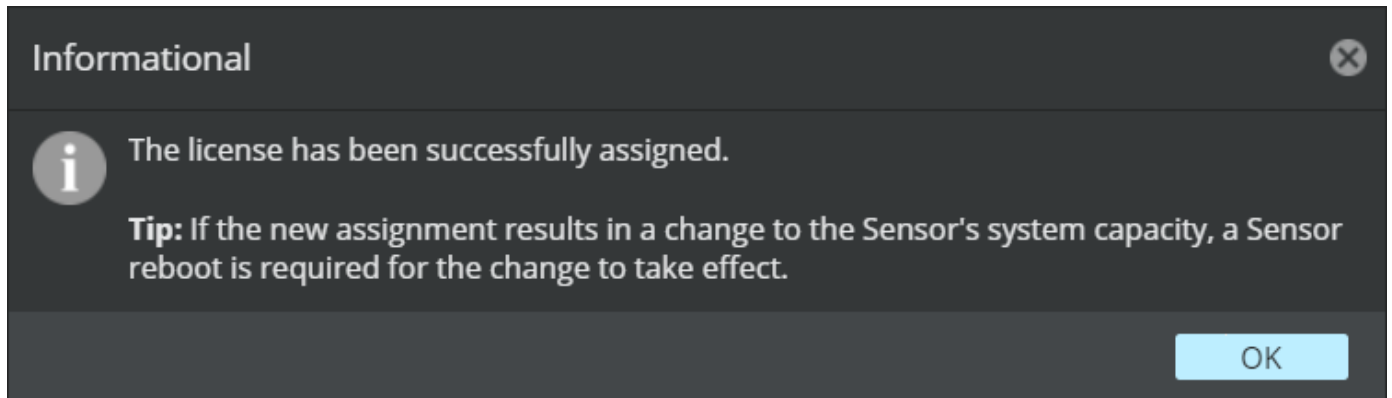
Assign To: /My Company/NS9500\_219

Assign

### Note

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

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



### Note

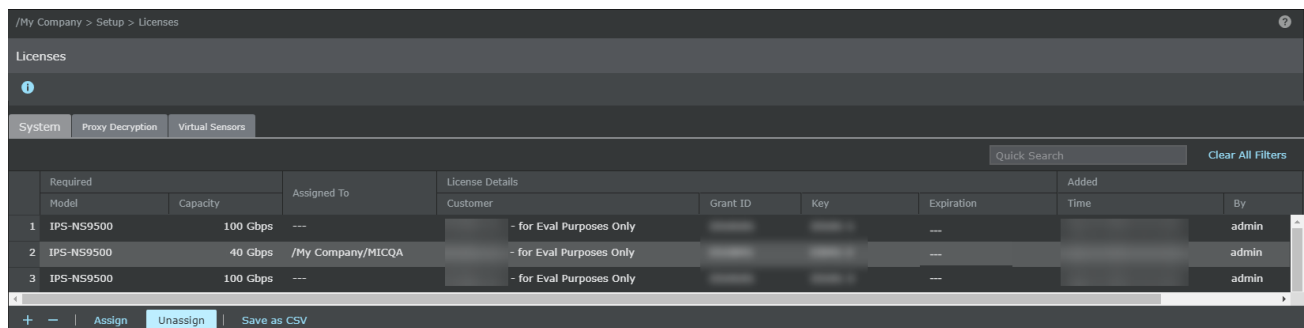
In case you are replacing an existing license with a license of varied capacity, you must reboot the device for the new capacity to take effect. If you are replacing an existing license with a same capacity license, reboot is not required.

:

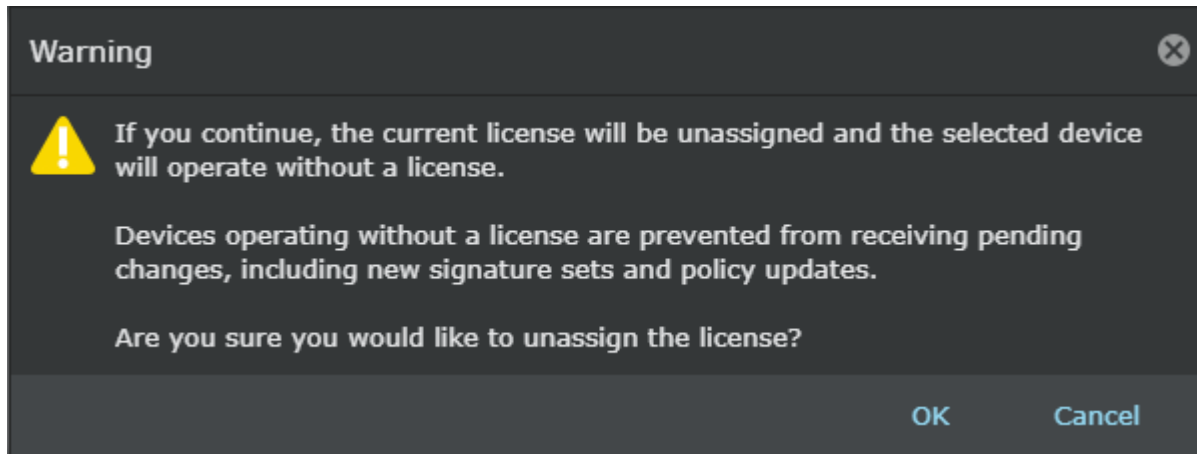
## Unassign a license from a Sensor

To unassign the license, perform the following steps:

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



4. Click Unassign.
5. Click Ok.



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

:

## Upgrade an existing capacity license

### Points for considerations:

Consider the following points before you upgrade the capacity license:

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

### Note

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



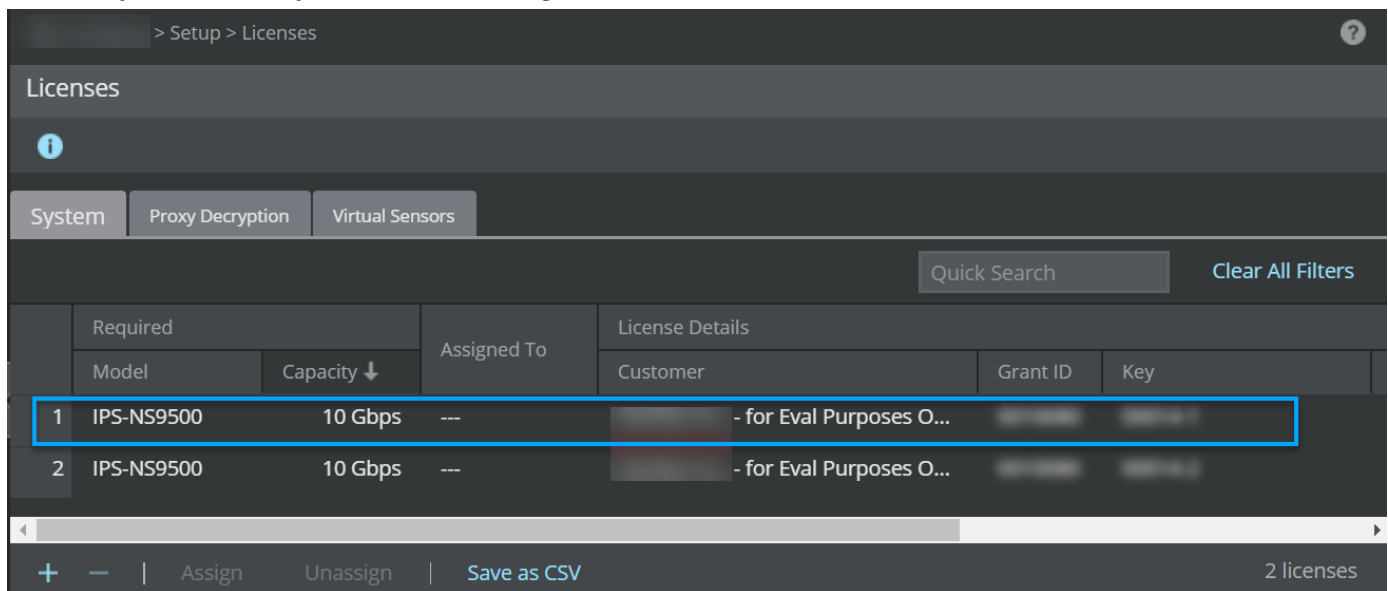
- If you do not have an existing license with x capacity, you cannot add an upgrade license with (x + y) capacity. For example, if you do not have a 10G license available in the Manager, you cannot add an upgrade license from 10G to 20G.....100G in the Manager.
- After the existing license (x) is replaced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

### Note

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

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

1. Go to Manager → <Admin Domain Name> → Setup → Licenses.
2. Click the System tab. The system tab with existing licenses:



Licenses						
Required		Assigned To	License Details			
Model	Capacity ↓		Customer	Grant ID	Key	
1	IPS-NS9500	10 Gbps	---	- for Eval Purposes O...		
2	IPS-NS9500	10 Gbps	---	- for Eval Purposes O...		

3. Click .

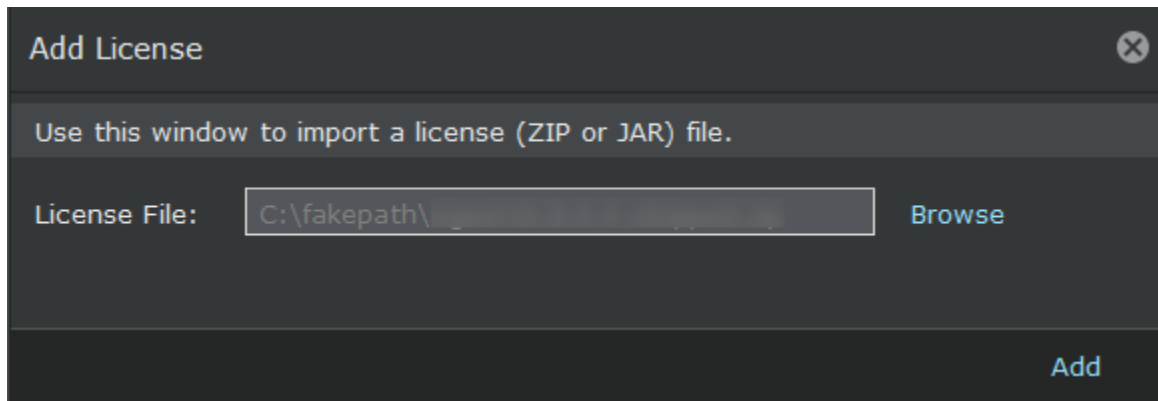
The Add License pop-up window opens.

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

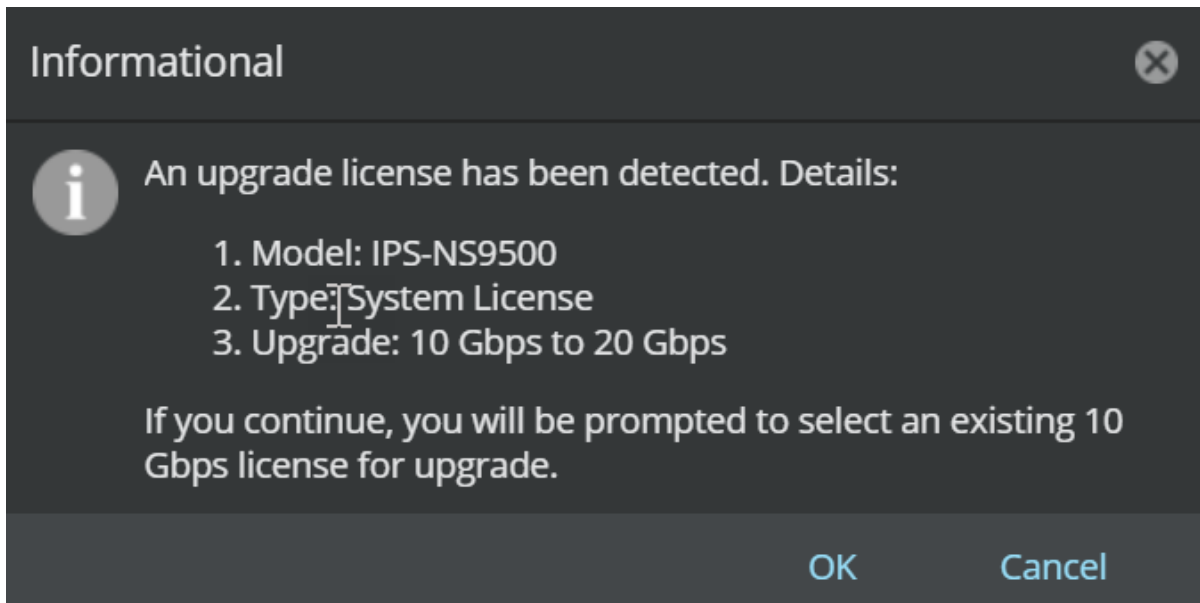
 Note

The supported license formats are zip and jar.

Upload license to the Manager

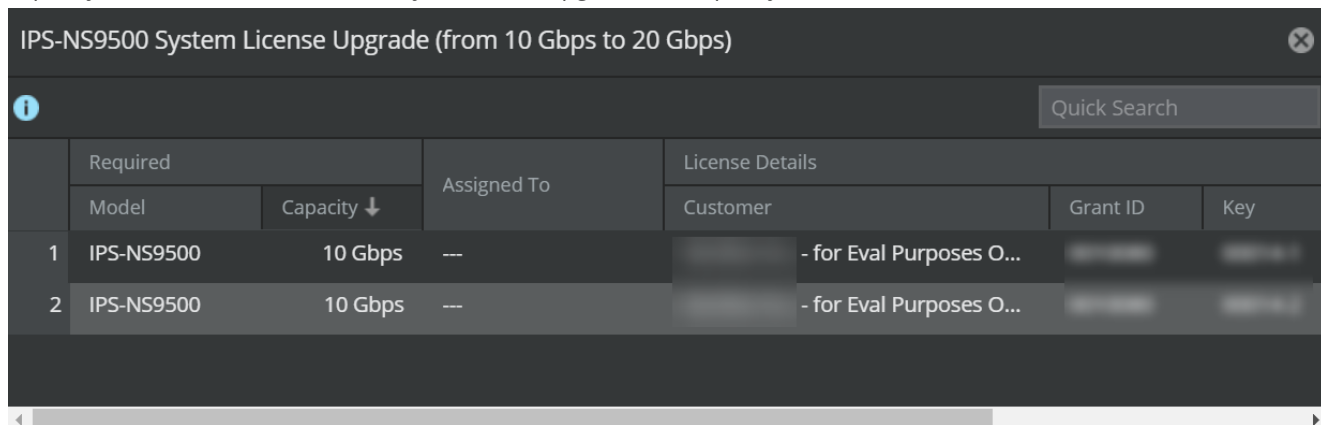


5. Click Add.
  - a. An informational message window appears. Click OK.

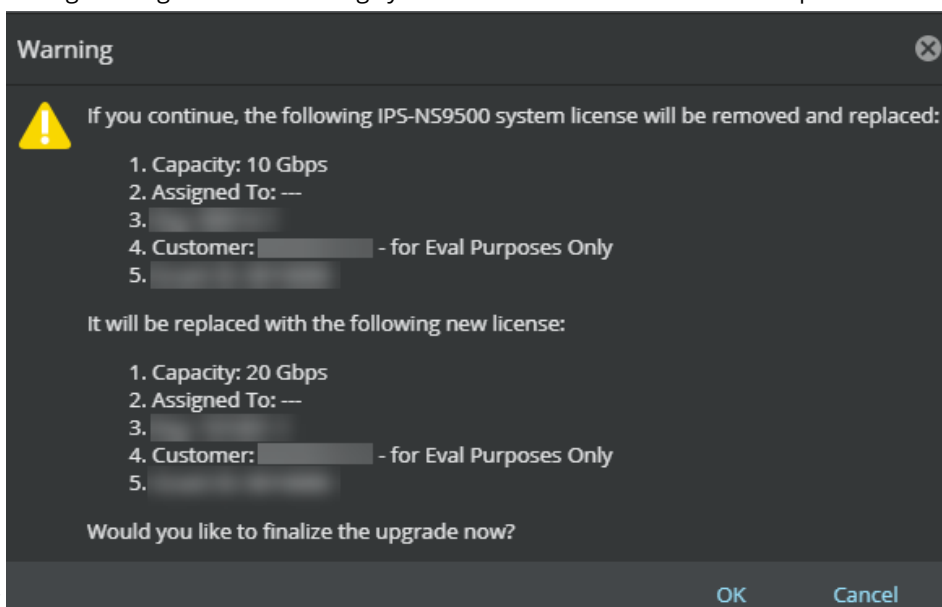


- b. <Sensor name> System license upgrade (from x Gbps to x+y Gbps) window appears which displays all the licenses present in the Manager for that particular

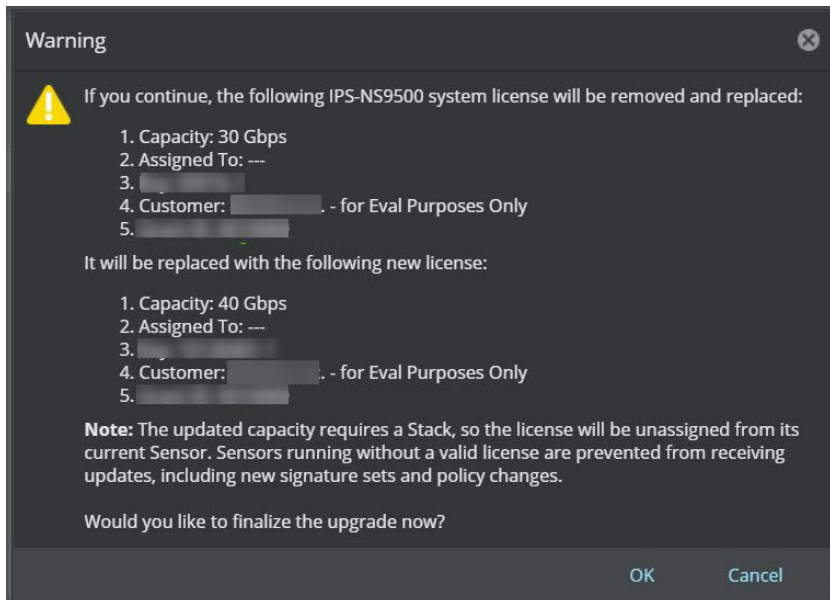
capacity. Double click on the license you wish to upgrade the capacity license for.



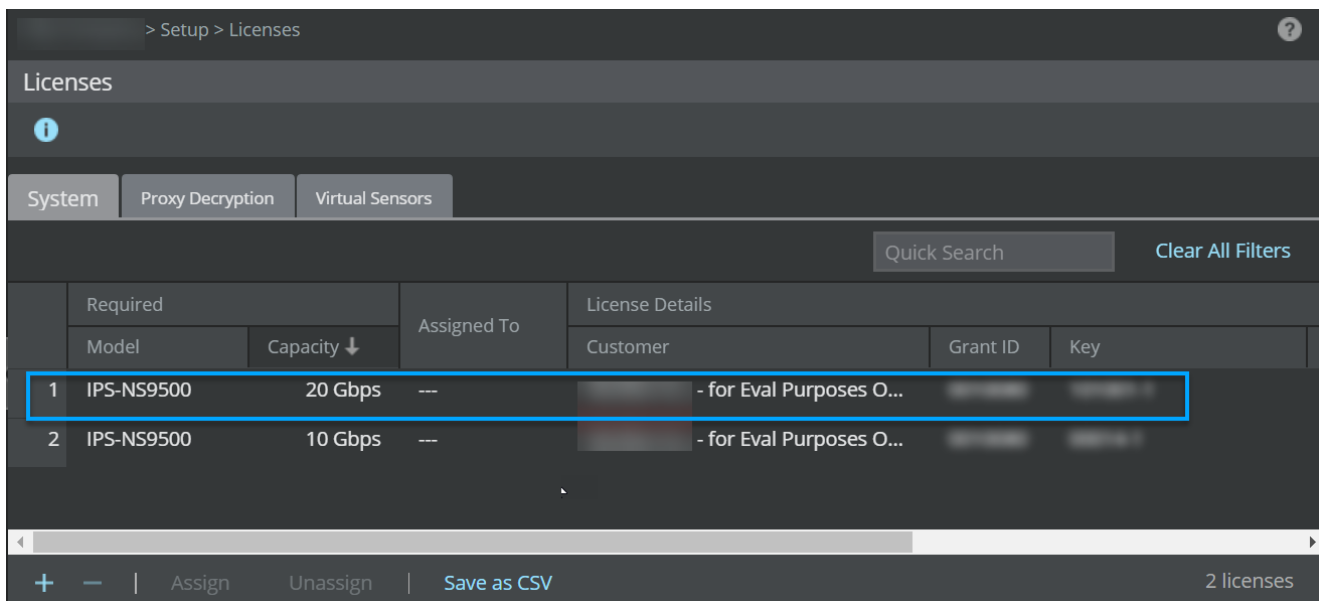
c. A warning message that the existing system license will be removed and replaced with a new license appears. Click



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



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



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

:

## Remove a license from the Manager

To remove a license, perform the following steps:

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

4. Click .

5. Click Ok. Once a license is removed from the Manager, you will not be able to deploy pending changes, update new signature sets and policy update to the Sensor from which the license is unassigned automatically upon deletion of the license.

:

## Stacking NS9500 Sensors

The NS9500 Sensor offers the solution of stacking multiple Sensors to achieve scalability. The individual Sensors in the stack are interconnected using external stacking cables. Stacking Sensors creates a unified data plane view across the stack. This allows the Manager to manage the stack as a unified device. In a stack, some of the Sensor properties like signature set and call back detector update etc. are managed at the stack level and remaining like port configuration, troubleshooting etc. are managed at the device level.

Even though the data plane is unified, some Sensor properties are managed at individual Sensor level from the Manager. Each Sensor in the stack has an independent connection to the Manager. The Manager interprets the stack as a collection of individual Sensors by creating a container entity called the stack.

Based on the requirement you can configure either 40 Gbps or 60 Gbps or 100 Gbps capacity for a stack. Separate licenses are required to achieve different capacity for the stack. Also, the number of Sensors required will vary based on the capacity. For more information, see [Considerations for stacking NS9500 Sensors](#).

:

### Considerations for NS9500 Sensor stack

For creating a stack of NS9500 Sensors, you need to take the following factors into consideration:

- Ensure that you have the required QSFP28 Direct Attach Copper (DAC) cables to create the stack.
- Sensor and licensing requirements

Capacity	Number of Sensors	License SKU
40 Gbps	2 NS9500 Sensors	NS95X40CAE-AT
60 Gbps	2 NS9500 Sensors	NS95X60CAE-AT
100 Gbps	4 NS9500 Sensors	NS95X100CAE-AT

- Unsupported features list:
  - SSL resumption for stack

- Configure packet capture settings in span port
- Proxy based Inbound and Outbound SSL decryption
- Import and export Sensor configuration
- Integration with NTBA
- Integration with EIA
- Denial of Service management, profiles, and filters
- Allocating interfaces at child domain

### Note

In the event of node failure in a stack, the remaining nodes will continue to function and a fault is generated in Manager → Troubleshooting → Logs → System Faults.

:

## Cable the Sensors in a standalone stack

This procedure describes how to cable Sensors in a stack.

1. Plug the QSFP28 Direct Attach Copper (DAC) cable into the port **G0/1** of the first Sensor.
2. Connect the other end of the cable into port labeled **G0/2** of the second Sensor.
3. In case of a 4 node stack, repeat steps 1 and 2 for the other Sensors in the stack.
4. To complete the stack, plug the QSFP28 Direct Attach Copper (DAC) cable into the port labeled **G0/2** of the first Sensor.
5. Connect the other end of the cable into port **G0/1** of the last Sensor.



6. On the rear panel of each NS9500 Sensor, plug a RJ-45 cable in the Management port (labeled MGMT).
7. Plug the other end of the cable into the network device connected to your Manager server.

 **Note**

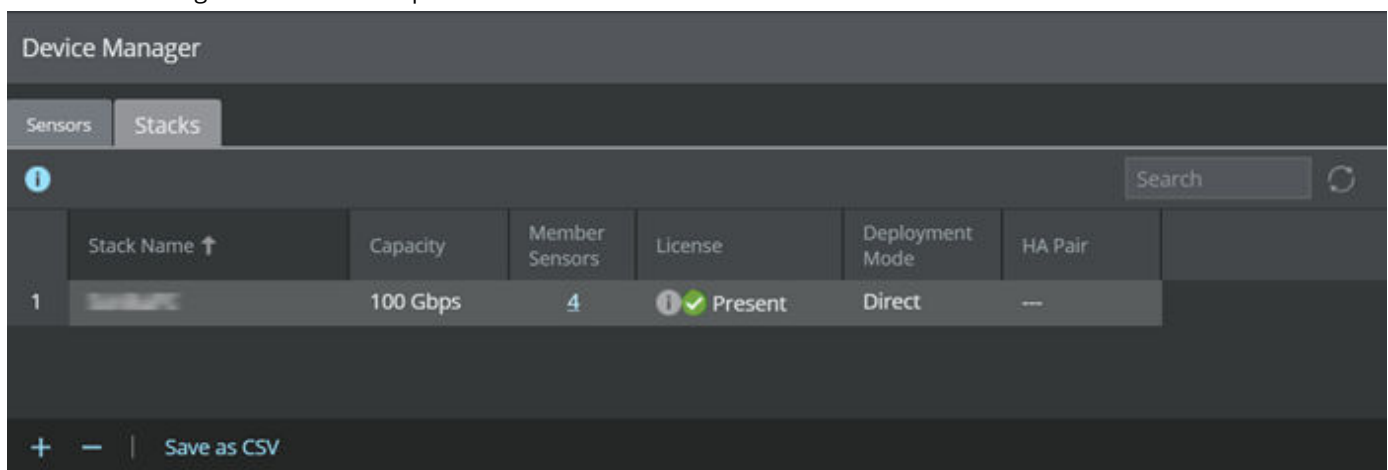
In a NS9500 Sensor standalone stack, you can connect one Sensor to another Sensor only by using a QSFP28 module.


:

## Add a stack to the Manager

The following steps describe how to add stacked Sensors to the Manager:

1. Start the Manager software.
2. Log in to the Manager (the default username is **admin** and the default password is **admin123**).
3. To add stacked Sensors in the Manager, click Devices → <Admin Domain> → Global → Device Manager, then click Manage Stacks. The Manage Stacks window opens.



4. Click  to add a new stack.  
The Stack Details window opens.

5. Enter the following mandatory information in the appropriate fields.

- Stack Name — The stack name must begin with a letter. The maximum length of the name is 25 characters.
- 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: ~ ` ! @ # \$ % ^ & \* ( ) \_ + - = [ ] { } \ | ; : " ' , . < ? /

#### Note

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

- Confirm Shared Secret — Confirm the shared secret key.
- Capacity — The throughput for the Stack. Based on the throughput, the number of Sensors will also differ. See the table below:

Capacity	Number of Sensors
40 Gbps	2
60 Gbps	2
100 Gbps	4



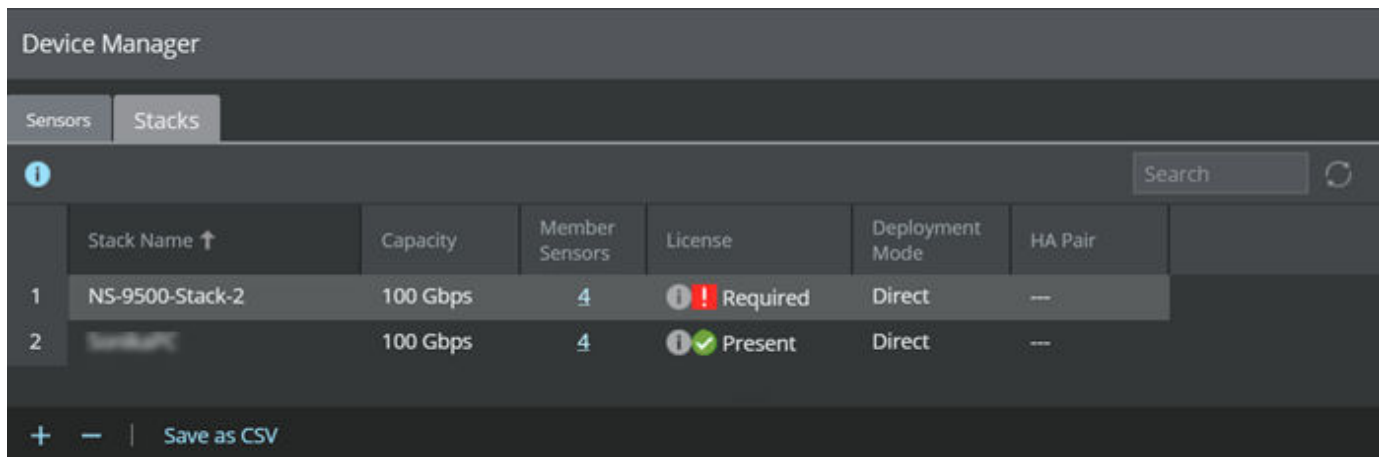
- Deployment Mode — Select Direct or Indirect.

 **Note**

Selecting Indirect enables Offline Sensor update. Direct is the default mode.

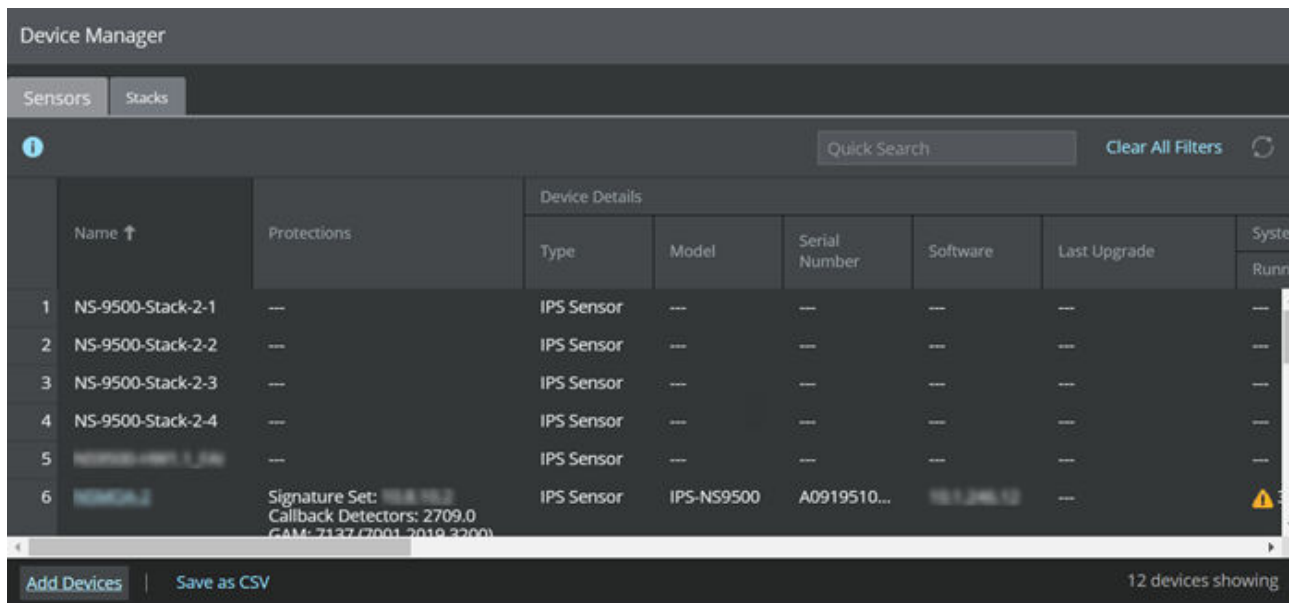
6. Click Save.

The new stack is displayed in the Manage Stacks window.



7. Close the Manage Stacks window.

In the Device Manager page, the member Sensor instances are displayed as <Stackname-node id> (for example, <Stackname-1>, <Stackname-2>, etc.) depending on the capacity.



Capacity	Sensor name
40 Gbps	<Stackname-1> <Stackname-2>
60 Gbps	<Stackname-1> <Stackname-2>
100 Gbps	<Stackname-1> <Stackname-2> <Stackname-3> <Stackname-4>

8. Using the Sensor CLI, configure the Sensors with the same name and node ID as the names displayed in the Device Manager page.
9. In the Manager, go to Manager → <Admin Domain> → Setup → Licenses and upload the license for the stack. You must manually push the configuration after the license is assigned to the stack. For more information on licenses, see [Managing licenses for NS9500 Sensors](#).

:

## 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.



**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.

1. Log in to the Sensor using the terminal connected to the Console port.
2. At the prompt, log in using the default Sensor username (**admin**) and password (**admin123**).

```

login as: admin
* * *

Authorized users only. Unauthorized users will be prosecuted
to the full extent of the law.

* * *
Using keyboard-interactive authentication.
Password:
Last login: Fri Sep 28 07:20:31 2012 from 172.16.230.77
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is 'off'.

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

```

- (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.

- Set the Sensor mode to stack or standalone based on your requirement using the **set sensor mode <stack | standalone>** command. You will be prompted to reboot the Sensor to change the mode. Press **Y** to confirm.
- 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.

- For a standalone Sensor, type: **set sensor name <word>** at the prompt. Example: **set sensor name HR\_sensor1**
- For Sensors in the stack, type **set stack name-node idat** at the prompt. Example: **set sensor name NS9500\_Stack-1**

#### 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.

You reset the Sensor to change the mode using the **resetconfig** command.

6. 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**
7. 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**
8. 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.

9. If prompted, reboot the Sensor. Type **reboot**

 **Note**

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

10. 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.
11. 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.

12. Type **show** to verify the configuration information. Check that all information is correct.
13. Type **exit** to exit the session.

:

## Considerations for failover in stacked Sensors

While configuring failover for a stack, you need to take the following factors into consideration:

- Both the stacks must be identical to each other with identical connections, network modules, and capacity.
- Ensure you have the correct license to configure failover for a stack. The licenses required are as follows:

Capacity	No of Sensors	Number of License SKUs
40 Gbps	2 * 2 NS9500 Sensors	FO95X40CAE-AT
60 Gbps	2 * 2 NS9500 Sensors	FO95X60CAE-AT
100 Gbps	2 * 4 NS9500 Sensors	FO95X100CAE-AT

- You can use 2-port QSFP28 interface module, or 2-port QSFP+ interface module or 4-port QSFP+ interface module for Sensor failover.
- Port G1/1 is used for failover. G1/2 is unusable. For 4-port interface module, ports G1/3 and G1/4 can be used as monitoring ports.
- You need to purchase separate Direct Attach Copper (DAC) cables for failover.
- The supported DAC cable length for the failover is 3 meters. It is recommended that the stack configuration is installed within one rack. If the stack is configured in multiple racks, you will need to use the QSFP+ SR fiber transceiver modules.

#### Note

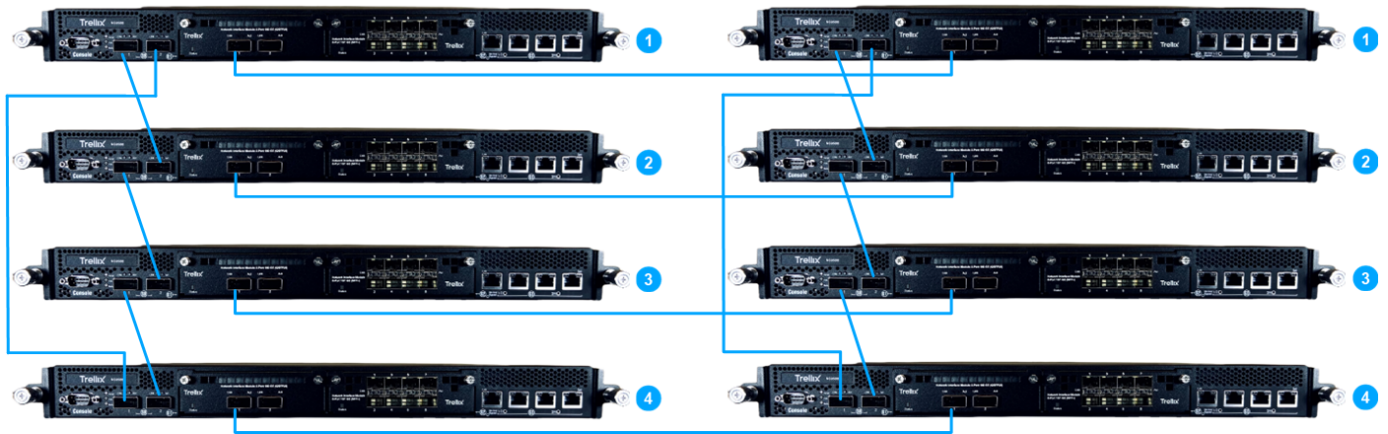
In the event of node failure in a stack, the remaining nodes will continue to function and a fault is generated in the System Faults page in the Manager.

:

### Cable the Sensors in a stack for high availability

This procedure describes how to cable Sensors in a stack for high availability.

1. Plug the QSFP28 Direct Attach Copper (DAC) cable into port **G1/1** or **G1/2** of the first Sensor in the primary stack.
2. Connect the other end of the cable into the corresponding port labeled **G1/1** or **G1/2** of the first Sensor in the secondary stack.
3. Repeat steps 1 and 2 for the other Sensors in the primary and secondary stack.



4. On the rear panel of each NS9500 Sensor, plug a RJ-45 cable in the Management port (labeled MGMT).
5. Plug the other end of the cable into the network device connected to your Manager server.
6. Create a failover pair using Manager's Failover Pairs page.

#### Note

To connect the first Sensor in the primary stack with the first Sensor in the secondary stack, you can use either the QSFP28 module (2x100 G) module or the QSFP+ (4x40 G) module. The QSFP28 modules support the DAC cables for interconnect.

:

## Scenarios for stacked NS9500 Sensors

This section explains about the scenarios for stacked NS9500 Sensors.

### Scenario 1: Node failure

#### Note

The examples in this section uses 4 node stack with 100 Gbps capacity. The scenarios are also valid for 2 node stack with 40 Gbps or 60 Gbps capacity.

In the event of a single or multiple node failure in a stack, the remaining Sensors continue to scan traffic and a fault is generated in the System Faults page in the Manager. You can view the status of the nodes in the stack in the Device Manager page.

#### Example 1: Single node failure



In this scenario, Node 2 in the stack becomes unresponsive. The remaining Sensors will continue to process traffic at a reduced throughput of 75 Gbps. Monitoring ports connected to the failed sensor will also experience failure. Trellix recommends you to use an Active Fail Open kit in such a scenario.

#### Example 2: Multiple node failure



In this scenario, nodes 2 and 4 in the stack becomes unresponsive. The remaining Sensors (node 1 and 3) will function as given below:

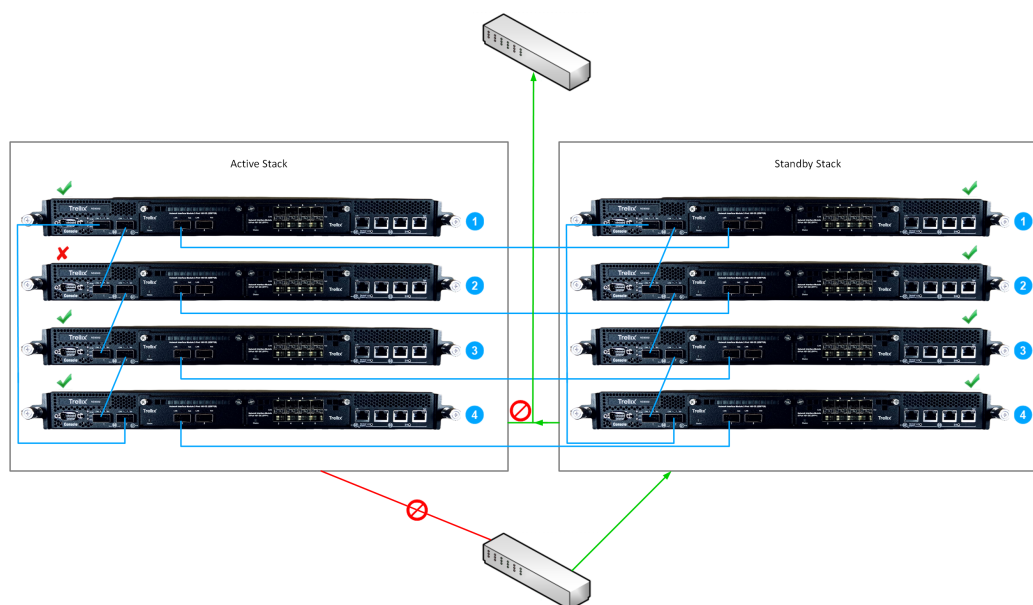
- If node 1 and node 3 are connected to the server, both nodes will continue to process traffic at 25 Gbps throughput as standalone Sensors.

- If only node 3 is connected to the server, node 3 will continue to process traffic at 25 Gbps throughput. Node 1 will be active but will not process traffic.

## Scenario 2: Node failure in a stack with failover

For stacked Sensor failover, heartbeat information is exchanged between the active and standby stack. This information contains the current capacity of both stacks. The traffic is processed by the stack that has the higher capacity. In the event of a node failure in the active stack, current capacity of the active stack will be less than the standby stack. In this case, the monitoring ports of the active stack will be deactivated and the traffic flows to the standby stack.

### Example 1: Single node failure in active stack

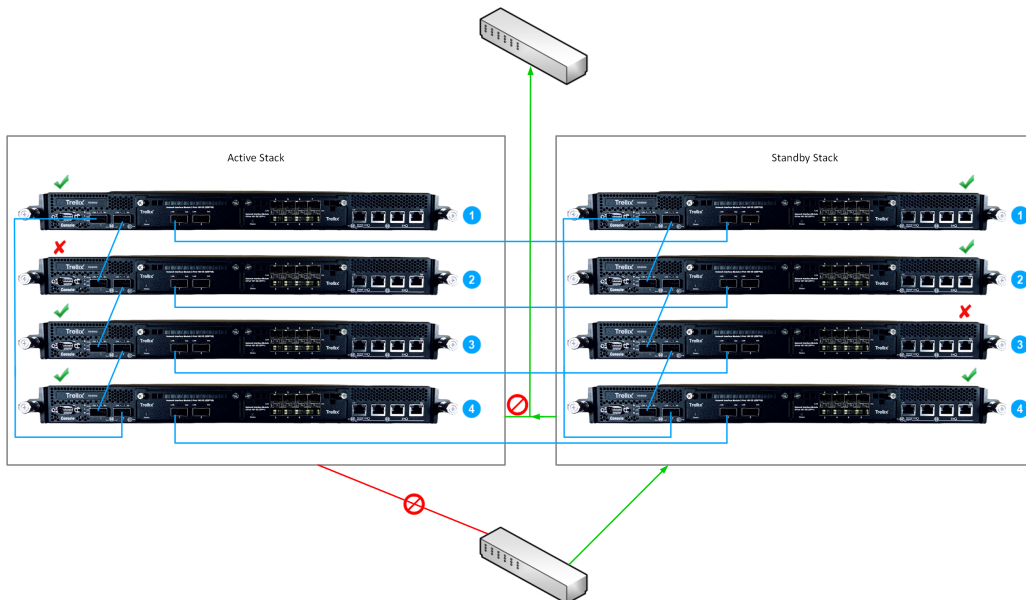


In this scenario, the workflow is as follows:

1. Node 2 in the active stack is not functional.
2. During the exchange of heartbeat information, the capacity of the active stack is lower than the standby stack.
3. When the active stack processes this information, the monitoring ports in the active stack is deactivated.
4. The standby stack takes over traffic inspection from the active stack.

### Example 2: Single node failure in active and standby stacks





In this scenario, the workflow is as follows:

1. Node 2 in the active becomes unresponsive.
2. During the heartbeat exchange between the stacks, the capacity of the of the active stack is lower that the standby stack.
3. The monitoring ports on the active stack is deactivated.
4. The standby stack starts processing the traffic.
5. Node 3 in the standby stack becomes unresponsive.
6. During the heartbeat exchange between the stacks, the capacity of the of the active stack is equal to the standby stack.
7. The standby stack continues to process the traffic.

#### Note

Switch over occurs only when the current capacity of standby stack is lower than the active stack.

:

## Configure the Sensor and Manager for deployment

:

### 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.


Steps:

1. Prepare the system according to the requirements outlined in *Trellix Intrusion Prevention System Installation Guide*.
2. Close all open applications.
3. Go to [Trellix Download Server](https://www.trellix.com/en-us/downloads/my-products.html) (<https://www.trellix.com/en-us/downloads/my-products.html>).
4. Log on using your **Grant Number** and registered **Email Address**.  
The Find Products page opens.
5. In the Category filter, select Network Security.
6. Click on the Manager version required.  
The Available Downloads page opens.
7. In the Type filter, select Installation.  
The Manager installation files available for download are listed.
8. Click on the required Manager installation file and the download starts.
9. Refer to *Trellix Intrusion Prevention System Installation Guide* for detailed procedure to install the Manager application.

:

## Add the Sensor to the Manager

Steps:

1. Log on to the Manager using the default user name (**admin**) and password (**admin123**).
2. Go to Devices → <Admin Domain Name> → Global → Device Manager.  
The Device Manager page is displayed.
3. 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.

4. Enter the following mandatory information in the appropriate fields:

- Name — The Sensor name must begin with a letter. The maximum length of the name is 25 characters.
- 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 enter later 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.

- Device Type — Specifies the type of device to be added. Select IPS Sensor.
- Deployment Mode — Select Direct or Indirect.

#### Note

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

- Contact Information — (Optional) Type the contact information.
- Location — (Optional) Type the location.
- Comment — (Optional) Type the comment.

5. Click Save.

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

:

## 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.



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.

### Steps:

1. Log on to the Sensor using the terminal connected to the Console port.
2. At the prompt, log on using the default Sensor username (**admin**) and password (**admin123**).

```
login as: admin
* * *

Authorized users only. Unauthorized users will be prosecuted
to the full extent of the law.

* * *
Using keyboard-interactive authentication.
Password:
Last login: Fri Sep 28 07:20:31 2012 from 172.16.230.77
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is 'off'.

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

3. (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.

4. Set the name of the Sensor.



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.

At the prompt, type: **set sensor name <word>**. Example: **set sensor name HR\_sensor1**



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.

5. 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**
6. 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**
7. 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**



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.

8. If prompted, reboot the Sensor. Type **reboot**



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

9. 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 that the information is correct.
10. 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.

11. Type **show** to verify the configuration information. Check that all information is correct.
12. Type **exit** to exit the session.

:

## Verify successful installation

### Steps:

1. Type **status** in the Sensor CLI. The status report appears.

```

intruShell@> status
[Sensor]
System Initialized      : yes
System Health Status   : good
Layer 2 Status         : normal (IDS/IPS)
Installation Status    : complete
IPv6 Status            : Dont Parse and Allow Inline
Reboot Status          : Not Required
Guest Portal Status    : up
Hitless Reboot         : Available
Last Reboot reason     : reboot issued from CLI

[Signature Status]
Present                : yes
Version               :
Power up signature     : good
Geo Location database  : Present
DAT file               : Present
DAT file Version      :

[Manager Communications]
Trust Established      : yes (Self Signed cert support)
Alert Channel         : up
Log Channel           : up
Authentication Channel : up
Last Error            : None
Alerts Sent           : 29254016
Logs Sent             : 27217316

[Alerts Detected]
Signature              : 29105690      Alerts Suppressed : 0
Scan                  : 12          Denial of Service : 132527
Malware                : 15807

[MATD Communication]
Status                : down
IP                    : 0.0.0.0
Port(Secure)         : 8505

```

The Sensor parameter **System Initialized** should be **yes**, and for Manager communication **Trust Established** should be **yes**.

2. Return to the Manager. In the Manager Home page, view the Manager status in the System Faults section. The Manager status should be up and Sensor status should be active.

System Faults				
Manager	Status	Critical	Error	Warning
Manager	Up	1	1	0
Device	Status	Critical	Error	Warning
_NS-series_Sensor_1	Active	6	0	3
_NS-series_Sensor_2	Active	4	1	3
NS9500_Stack-1	Unknown	0	0	0
NS9500_Stack-2	Unknown	0	0	0
_Sensor_1	Active	0	0	0
_Sensor_2	Active	1	0	0
_VM600_1	Active	0	0	0
_VM600_2	Active	0	0	0

- From the Manager Home page, click Configure to open the Configuration page.
- Select your added Sensor: Device List → <Device\_Name>. The ports for this Sensor appear under the <Device\_Name> node.

### Note

<Device\_Name> indicates the name of the Sensor you added.

Physical Ports					
Port	Link	Virtual Adapter	Operation Mode	Placement	Response Port
I/O Module: G0 (2-port Q5FP+ module detected)					
0/1	---	---	---	---	---
0/2	---	---	---	---	---
I/O Module: G1 (empty)					
---	---	---	---	---	---
I/O Module: G2 (empty)					
---	---	---	---	---	---
I/O Module: G3 (8-port RJ-45 module detected)					
3/1	⊘ Disabled		In-line Fail Open (Paired with 3/2)	Inside Network	This Port
3/2	⊘ Disabled		In-line Fail Open (Paired with 3/1)	Outside Network	This Port
3/3	✔ Up		In-line Fail Open (Paired with 3/4)	Inside Network	This Port
3/4	✔ Up		In-line Fail Open (Paired with 3/3)	Outside Network	This Port
3/5	✔ Up		In-line Fail Open (Paired with 3/6)	Inside Network	This Port
3/6	✔ Up		In-line Fail Open (Paired with 3/5)	Outside Network	This Port
3/7	⊘ Disabled		In-line Fail Open (Paired with 3/8)	Inside Network	This Port
3/8	⊘ Disabled		In-line Fail Open (Paired with 3/7)	Outside Network	This Port

- 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 IPS-provided policies, you can clone the policy and then customize it as described in *Trellix Intrusion Prevention System Product Guide*.

6. Click Device List → <Device\_Name> → Port Settings.
7. 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*.

:

## You're up and running!

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

### Steps:

1. For detailed usage instructions, see *Trellix Intrusion Prevention System Product Guide*, or click the ? buttons in the upper-right corner of each window in the Manager.
2. Start the Analysis → <Admin Domain> → Attack Log to view alert statistics as attacks are detected. A summary of alerts is displayed in the Unacknowledged Alert Summary monitor of the Manager Dashboard page.
3. Having problems? Check *Trellix Intrusion Prevention System Product Guide* for troubleshooting information.
4. 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://supportm.trellix.com>.

:

## Troubleshooting the Sensor

This section lists some common installation problems, the possible causes, and the corresponding solutions.

Problem	Possible Cause	Solution
LED is off.	The Sensor is turned off.	Restore Sensor power.



<b>Problem</b>	<b>Possible Cause</b>	<b>Solution</b>
LED is off.	The Sensor port cable is disconnected.	Check the Sensor cable connections.
Sensor is operational but is not monitoring traffic.	Network device cables have been disconnected.	Check the cables and make sure they are properly connected to both the network devices and the bypass switch.
Sensor is operational but is not monitoring traffic.	The Sensor ports have not been enabled in the Manager.	The Sensor will not monitor traffic on the ports unless the ports are enabled in the Manager. Ports are disabled in case of Sensor failure; you must re-enable them for Sensor monitoring to resume.
Network or link problems	Improper cabling or port configuration	Make sure that the transmitting and receiving cables are properly connected to the bypass switch.
Runts or giants errors on switch and routers	Improper cabling or port configuration	Make sure that the transmitting and receiving cables are properly connected to the bypass switch.
The system fault "Switch absent" appears in the Manager Status page.	The Active Fail-Open Kit is disconnected.	Check the Active Fail-Open Kit and make sure it is properly connected to the Sensor.

:

## Sensor technical specifications

The following table lists the specifications of for NS9500 Sensors.

Sensor Specifics	NS9500
Dimensions	17 ¼" (W) x 29 1/16" (D) x 1 ¾" (H)
Weight	28.55 lbs
Storage	2 x 240 GB M.2 drive
<b>System Heat Dissipation</b>	
Maximum BTU	2038 BTU/hr
Typical BTU	1790 BTU
Maximum Power Consumption	598 W
Typical Power Consumption	525 W
Redundant Power Supply	Yes
Power	100 - 240 VAC (50 - 60 Hz)
DC Power Supply	<p>Installing DC power supply is optional.  Maximum Power Consumption: 598 W  Maximum BTU: 2038 BTU/hr  Power Supply Unit:</p> <ul style="list-style-type: none"> <li>• Input V: - 40 to -72 V</li> <li>• Input A: 12.45 A</li> </ul>
Temperature	Operating: 0° to 35° C , Non-operating: - 40° to 70° C
Relative humidity (non-condensing)	Operational: 10% to 90%, Non-operational: 5% to 95%
Altitude	0 to 10,000 feet
Safety Certification	UL 60950-1 (USA); CSA 22.1.No. 60950-1 (Canada); EN 60950-1 (Europe); CNS 14336-1 (Taiwan), GB

<b>Sensor Specifics</b>	<b>NS9500</b>
	4943-1 (China); IEC 60950-1 (International) - CB Scheme certificate and test report covering all applicable country deviations; IEC 60825 and 21CFR1040
<b>EMI Certification</b>	FCC Part 15 Subpart B Class A (USA); CAN ICES-3 Class A (Canada); EN 55022, EN 55032, EN 55024, EN61000-3-2, EN61000-3-3 (Europe and International); VCCI Class A (Japan); AS/NZS CISPR 32 (Australia and New Zealand); CNS 13438 (Taiwan); GB 9254-2008 (China); KN32 and KN35 (South Korea); GB 17625.1 (China)

:

## NS9x00 Sensors

:

### About Sensors

Sensors are high-performance, scalable, and flexible content processing appliances built for the accurate detection and prevention of:

- Network intrusions
- Network misuse
- Distributed Denial-of-Service (DDoS) attacks

Sensors are specifically designed to handle traffic at wire speed, efficiently inspect and detect intrusions with a high degree of accuracy, and flexible enough to adapt to the security needs of any enterprise environment. When deployed at key network access points, the Sensor provides real-time traffic monitoring to detect malicious activity and respond to such activity based on the responses configured by the administrator.

After you deploy a Sensor successfully, you configure and manage it using the Manager. The process of configuring a Sensor and establishing communication with the Manager is described in subsequent chapters of this guide. For the details about the Manager, see the *Manager Administration* section in *Trellix Intrusion Prevention System Product Guide*.

:

### Functions of an NS-series Sensor

The NS-series Sensors are a third-generation hardware platform for Sensors designed for high bandwidth links to offer Next Generation IPS (NGIPS) capability and provide high aggregate throughput across various Sensor models. The following models are supported.

- NS9300 - The NS9300 Sensor consists of a Primary Sensor and a Secondary Sensor. Each of these is a 2RU unit, providing an aggregate throughput of 40 Gbps.
- NS9200 - The NS9200 Sensor is a 2RU unit providing an aggregate throughput of 20 Gbps.
- NS9100 - The NS9100 Sensor is a 2RU unit providing an aggregate throughput of 10 Gbps.

The primary function of a Sensor is to analyze traffic on selected network segments and to respond when an attack is detected. The Sensor examines the header and data portion of every network packet, looking for patterns and behavior in the network traffic that indicate malicious activity. The Sensor examines packets according to user-configured policies, or rule sets, which determine what attacks to watch for, and how to respond with countermeasures if an attack is detected.

If an attack is detected, a Sensor responds according to its configured policy. Sensor can perform many types of attack responses, including generating alerts and packet logs, resetting TCP connections, "scrubbing" malicious packets, and even blocking attack packets entirely before they reach the intended target.

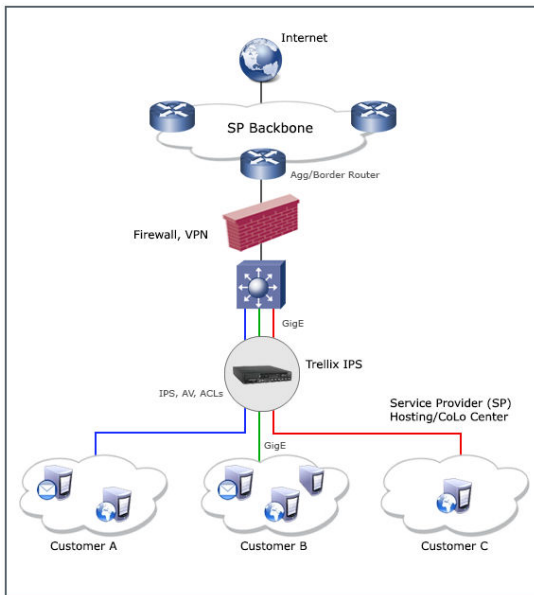
:

## Deployment of an NS-series Sensor

Deployment of a Sensor requires knowledge of your network to help determine the level of configuration and the number of installed Sensors. You also need to determine the number of Trellix ePolicy Orchestrator - On-prem servers required to protect your network. The Sensor is purpose-built for the monitoring of traffic across one or more network segments.

Following is an example of a network topology using Gigabit Ethernet throughput. In the illustration, Trellix Intrusion Prevention System provides IPS protection to outsourced servers. High port-density and virtualization provides a highly scalable solution, while Trellix IPS protects against web and eCommerce mail server exploits.

### A sample NS-Series Sensor deployment



:

## NS-series physical description

The high-port density NS-series Sensor is designed for high bandwidth links. This section gives a physical description of the NS-series Sensor.

:

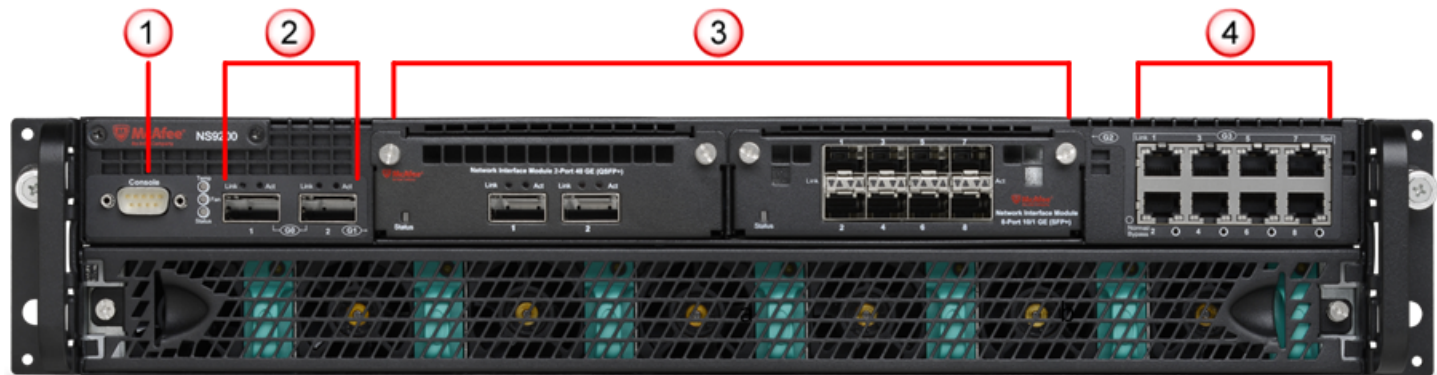
### Components of an NS-series Sensor

## The Sensor front panel

Correlate the pictures with the information following it to understand the components of an NS-series Sensor.

### The NS9100/NS9200 Sensor model

Sensor front panel

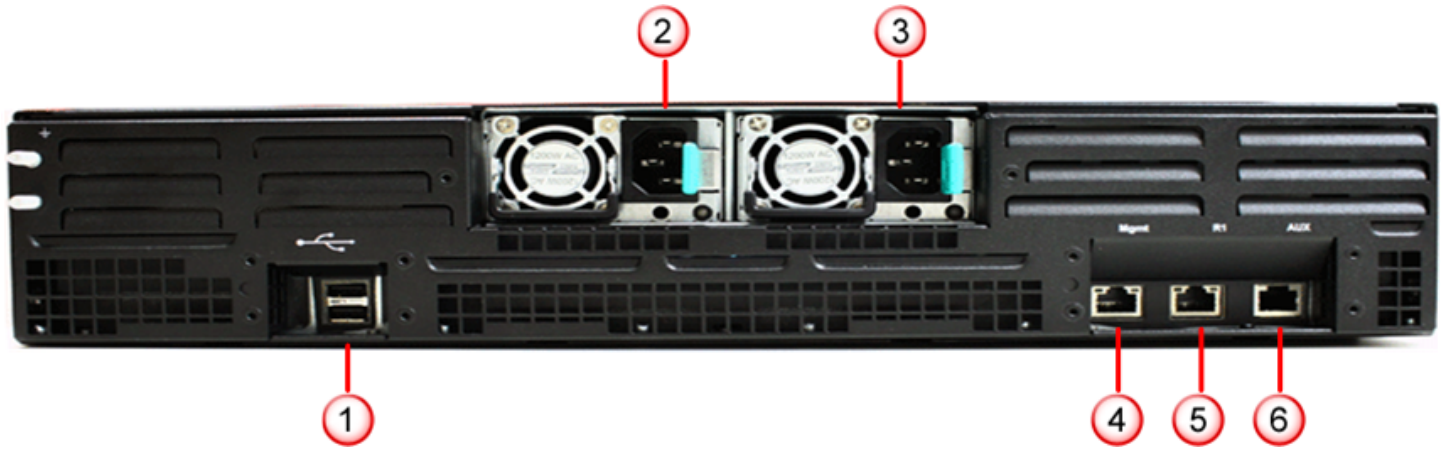


1. Console port (1)
2. QSFP+ 40 Gigabit Ethernet ports (2)
3. Two slots for I/O modules (Any combination of the interface modules can be used)
  - QSFP+ 40 Gigabit Ethernet ports (4)
  - QSFP+ 40 Gigabit Ethernet ports (2)
  - SFP/SFP+ 1/10 Gigabit Ethernet Monitoring ports (8)
  - RJ-45 10/100/1000 Mbps Ethernet Monitoring ports (6)
4. RJ-45 10/100/1000 Mbps Ethernet Monitoring ports (8)

The supported transceiver modules are QSFP+, SFP+ (M2M and SM), SFP Fiber (MM and SM) and SFP Copper.

Sensor rear panel

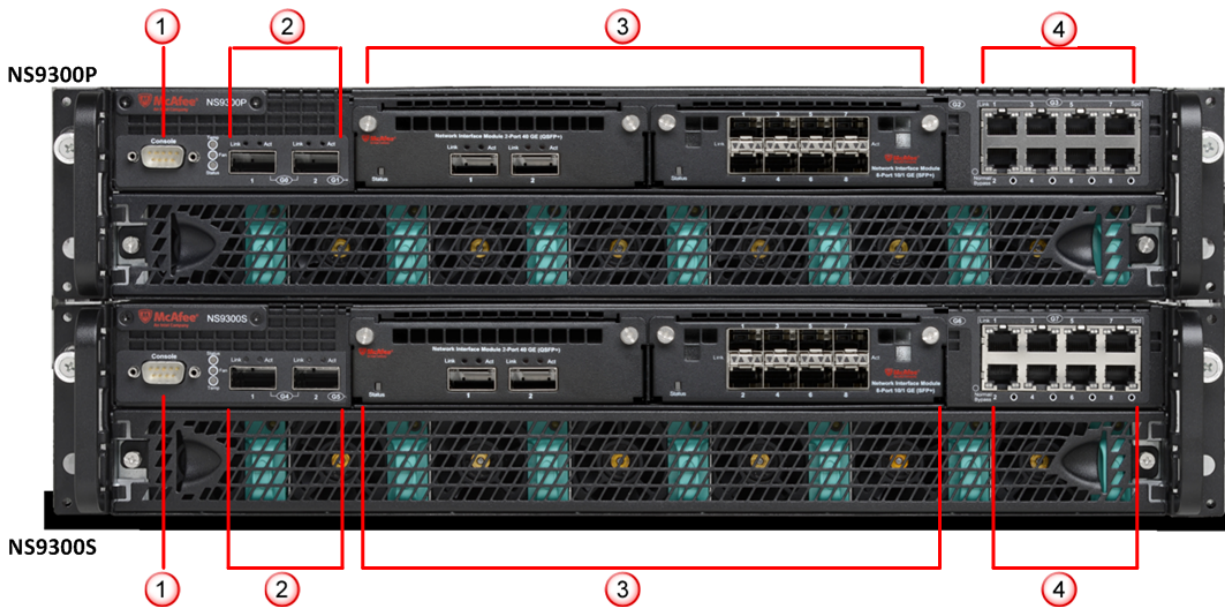
---



1. USB ports (2)
2. Power supply A (Pwr A)
3. Power supply B (Pwr B)
4. RJ-45 100/1000/10000 Management port (Mgmt) (1)
5. RJ-45 100/1000/10000 Response port (R1) (1)
6. RJ-45 Auxiliary port (Aux) (1)

### The NS9300 Sensor model

Sensor front panel

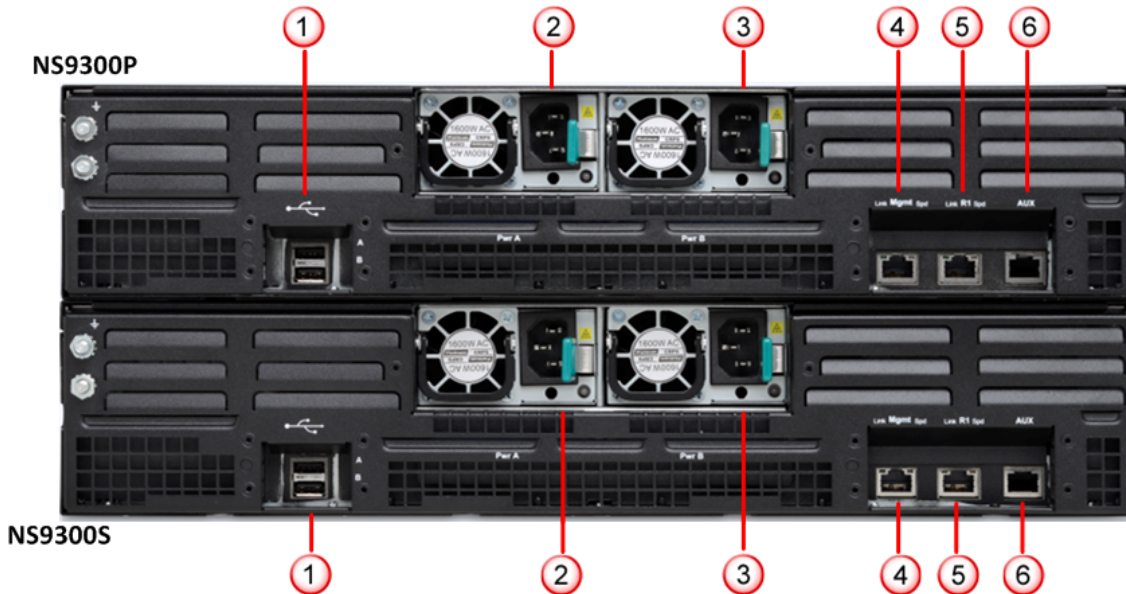


The **NS9300** Sensor consists of a Primary Sensor, **NS9300P**, and a Secondary Sensor, **NS9300S**.

1. Console ports on the NS9300P and NS9300S Sensors (2)
2. QSFP+ 40 Gigabit Ethernet Interconnect ports (4). G0/1 and G0/2 on NS9300P Sensor and G4/1 and G4/2 on NS9300S Sensor.
3. Four slots for I/O modules (Any combination of the interface modules can be used)
  - QSFP+ 40 Gigabit Ethernet ports (4)
  - QSFP+ 40 Gigabit Ethernet ports (2)
  - SFP/SFP+ 1/10 Gigabit Ethernet Monitoring ports (8)
  - RJ-45 10/100/1000 Mbps Ethernet Monitoring ports (6)
4. RJ-45 10/100/1000 Mbps Ethernet Monitoring ports (16)

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

Sensor rear panel

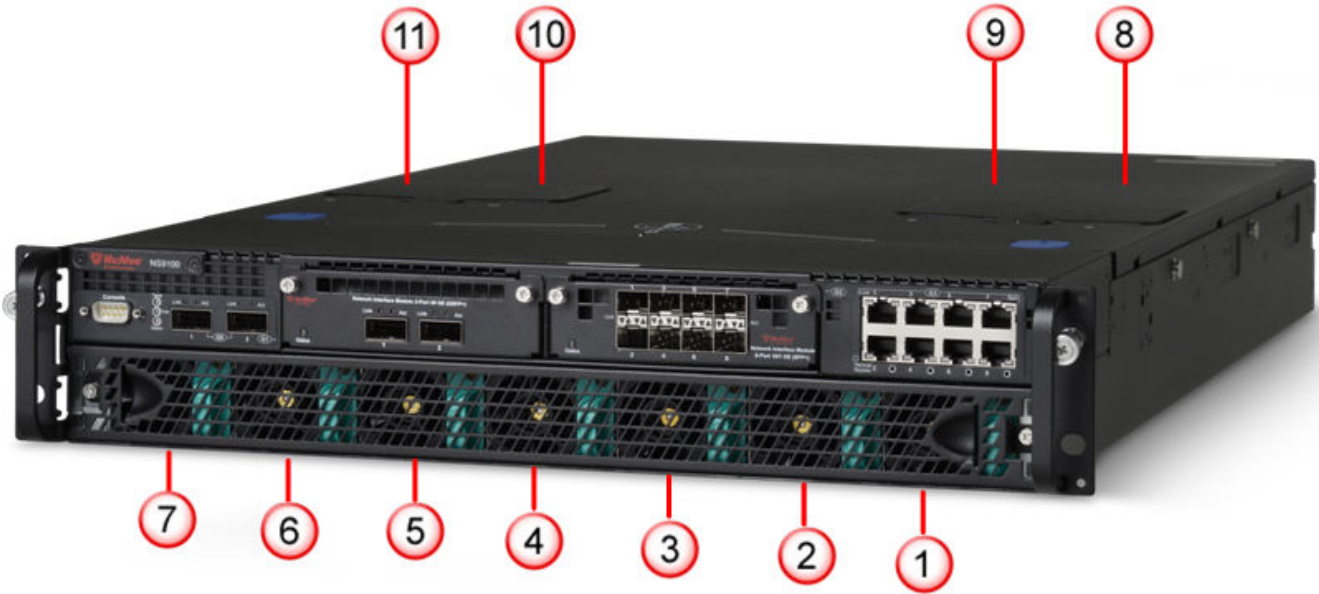


1. USB ports (4)
2. Power supply A (Pwr A)
3. Power supply B (Pwr B)
4. RJ-45 100/1000/10000 Management port (Mgmt) (2). Mgmt on NS9300S Sensor is used as an interconnect port.
5. RJ-45 100/1000/10000 Response port (R1) (2). R1 on NS9300P Sensor is used as an interconnect port.
6. RJ-45 Auxiliary ports (Aux) (2)

The NS9100 and NS9200 Sensors have seven fan units on the front panel and four fan units on the top.

Fan units-NS9100/NS9200

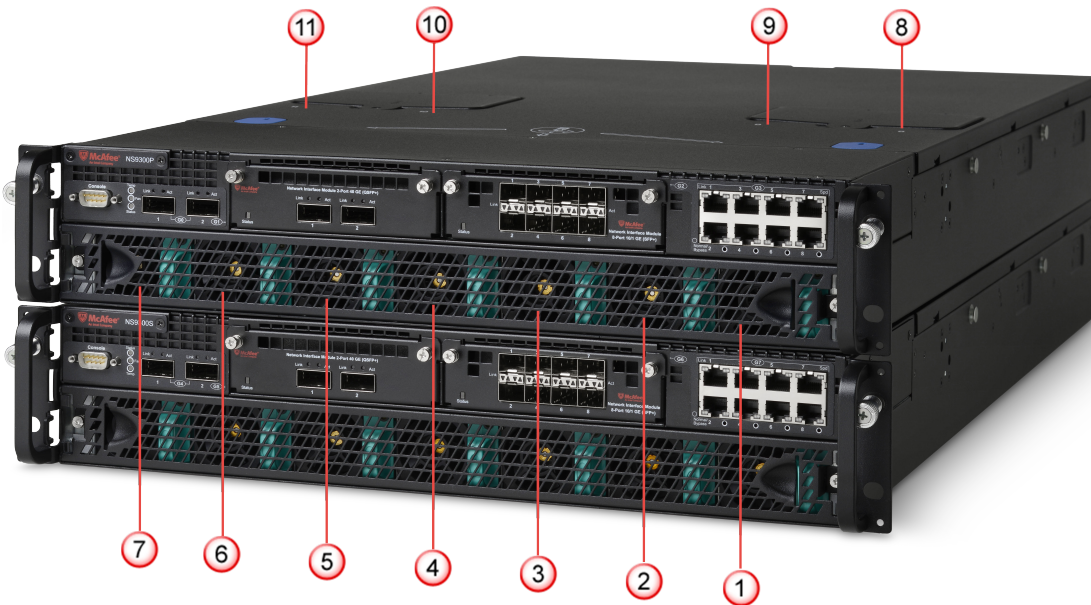




The NS9300 Sensors have seven fan units each for the primary and secondary Sensors on the front panel, and four fan units each for the primary and secondary Sensors on the top.

The direction of airflow in all the Sensors is front to back. Cold air enters through the front of the chassis.

Fan units-NS9300



 **Note**

The fan units and power supplies of NS9100, NS9200, and NS9300 are field replaceable and hot swappable.

The following table gives the details of the supported ports.

Ports	NS9100/NS9200	NS9300
Fixed Gigabit Ethernet—Copper Ports (internal fail-open)	8	16
Fixed 40-Gigabit Ethernet	2	4 (used as interconnect ports between NS9300P and NS9300S )
Network I/O Slots	2	4
Network I/O Modules (four options)	8 port (SFP+/SFP) 10 GigE/1 GigE 6 port RJ-45 10/100/100 Mbps 2 port (QSFP+) 40 GigE 4 port (QSFP+) 40 GigE	8 port (SFP+/SFP) 10 GigE/1 GigE 6 port RJ-45 10/100/100 Mbps 2 port (QSFP+) 40 GigE 4 port (QSFP+) 40 GigE
10 Gigabit Ethernet	Modular up to 16	Modular up to 32
40-Gigabit Ethernet	Modular up to 8	Modular up to 16
10/100/100 Mbps	Modular up to 12	Modular up to 24
Dedicated Response Ports (RJ45)	1 (10G/1G/100M)	1 (10G/1G/100M) on NS9300S
Dedicated Management Ports (RJ45)	1 (10G/1G/100M)	1 (10G/1G/100M) on NS9300P
Dedicated Auxillary Port (RJ45)	1 (10G/1G/100M)	2 (10G/1G/100M)
USB ports	2	4

- **RJ-45 10/100/1000 Management port**, which is used for communication with the Manager server. You can assign an IP address to this port during installation. These ports have built-in fail-open function.
- **Console port**, which you use to set up and configure the Sensor using the CLI.

- **RJ-45 Auxiliary port**, which you might use to dial in remotely to set up and configure the Sensor.
- **QSFP+ 40 Gigabit Ethernet Monitoring ports**, which enable you to monitor four SPAN ports, two segments in-line, or a combination.
- **SFP/SFP+ 1/10 Gigabit Ethernet Monitoring ports**, which enable you to monitor eight SPAN ports, four segments in-line, or a combination.
- **RJ-45 10/100/1000 Mbps Ethernet Monitoring ports**, which enable you to monitor eight SPAN ports, four segments in-line, or a combination.

### Note

- These Monitoring interfaces of the NS-series Sensor work in stealth mode, meaning they have no IP address and are not visible on the monitored segment.
- The gigabit ports of the Sensor running in in-line mode fail-close, meaning that if the Sensor fails, it will interrupt/block data flow. Fail-open functionality requires either the Layer 2 Passthru feature, described in detail in the *IPS Administration* section of *Trellix Intrusion Prevention System Product Guide* or the hardware Gigabit Fail-Open Bypass kit for gigabit ports.

**RJ-45 100/1000/10000 Response port**, which enables you to inject response packets back through a switch or router when you're operating in SPAN or tap mode.

- **External USB ports**. You use this in troubleshooting situations for system recovery purposes. You need to restart the Sensor through the USB storage device.
- **Primary Power Supply-A** (included). Power supply A is included with an NS-series Sensor. The supply uses a standard IEC port (IEC320-C13). Trellix provides a standard, 2m NEMA 5-15P (US) power cable (3 wire). International customers must procure a country-appropriate power cable.
- **Power Supply-B** (included). Power supply B is a hot-swappable, redundant power supply. This power supply also uses a standard IEC320-C13 port, and you can use the Trellix-provided cable or acquire one that meets your specific needs.

The NS-series Sensor does not have internal taps; you must use it with a third-party external tap to run it in tapped mode.

:

## Sensor LEDs

The front and rear panel LEDs provide status information for the health of the Sensor and the activity on its ports. The following table describes the NS-series LEDs.

## Front panel LEDs

LED	Status	Description
Status	Green Amber	Sensor is operating in good health. Sensor is booting up. It also indicates system bad health.
Fan	Green Amber	All three fans are operating. One or more fans are not working.
Temp	Green Amber	Inlet air temperature measured inside the chassis is normal. (Chassis temperature OK) Inlet air temperature measured inside the chassis is too high. (Chassis temperature too hot)
Gigabit Ports Act	Blinking Amber Off	Data is received or transmitted. No data is being transferred.
Gigabit Ports Link	Green Off	The link is up. The link is down.
RJ45 FailOpen/Bypass	Green Off	The port pair is in Inline Fail-Open/Inline Fail-Close/SPAN/Tap Mode. The Port Pair is in the Bypass Mode.

## Rear panel LEDs

LED	Status	Description
Pwr A (Power A)	Solid Green Blinking Green Solid Amber	Power Supply A is functioning. Power Supply A is stand-by. It also indicates load sharing. Power Supply A is not functioning or the unit has no power feed.
Pwr B (Power B)	Solid Green Blinking Green Solid Amber	Power Supply B is functioning. Power Supply B is stand-by. It also indicates load sharing. Power Supply B is not functioning or the unit has no power feed.
Management Port Speed	Green Amber Off	The port speed is 10000 Mbps. The port speed is 1000 Mbps. The port speed is 100 Mbps.
Management Port Link	Green Off	The link is up. The link is down.
Response Port Speed	Green Amber Off	The port speed is 10000 Mbps. The port speed is 1000 Mbps. The port speed is 100 Mbps.
Response Port Link	Green Off	The link is up. The link is down.

:

## Before you install

This chapter describes the best practices for deployment of Sensors in your network. Topics include the safety considerations for handling the Sensor, usage restrictions that apply to the Sensor model, and the contents that are shipped along with the Sensor.

:

## Usage restrictions

The following restrictions apply to the use and operation of a Sensor:

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

:

## Safety measures

Please read the following warnings before you install the Sensor. These safety measures apply to all Sensor models unless otherwise noted. Failure to observe these safety warnings could result in serious physical injury.

### Warnings:

- Read the installation instructions before you connect the system to its power source.
- To remove all power from the Sensor, unplug all power cords, including the redundant power cord.
- Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
- Before working on the equipment that is connected to power lines, remove all jewelry including rings, necklaces, and watches. Metal objects will heat up when connected to power and ground, and can cause serious burns or weld the metal object to the terminals.
- This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.
- Do not remove the outer shell of the Sensor. Doing so will invalidate your warranty.
- Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Blank faceplates and cover panels prevent exposure to hazardous voltages and currents inside the chassis, contain electromagnetic interference (EMI) that might disrupt other equipment and direct the flow of cooling air through the chassis.
- To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the users will be required to correct the interference at their own expense.
- Refer to the Appendix for information on regulatory, compliance, and other safety requirements.

:

## About fiber-optic ports

The Sensor uses fiber-optic connectors for its Monitoring ports. The connector type is an SFP/SFP+/QSFP+ fiber optic connector that is LC-duplex compatible.

Note the following:

- Fiber-optic ports (for example, SFP/SFP+/QSFP+, FDDI, OC-3, OC-12, OC-48, ATM, GBIC, and 100BaseFX) are considered Class 1 laser or Class 1 LED ports.
- These products have been tested and found to comply with Class 1 limits of IEC 60825-1, IEC 60825-2, EN 60825-1, EN 60825-2, and 21CFR1040.

### Caution

To avoid exposure to radiation, do not stare into the aperture of a fiber-optic port. Invisible radiation could be emitted from the aperture of the port when no fiber cable is connected.

- Only FDA registered, EN 60825-1 and IEC 60825-1 certified Class 1 SFP/SFP+/QSFP+ laser transceivers are acceptable for use with the Sensor.

:

## Contents of 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
- 40G Direct Attach cable

:

## Unpack the Sensor

Steps:

1. Open the crate.
2. Remove the first accessory box.
3. Verify you have received all parts. These parts are listed on the packing list and in *Contents of the box* section.
4. Remove the Sensor.
5. Place the Sensor box as close to the installation site as possible.

6. Position the box with the text upright.
7. Open the top flaps of the box.
8. Remove the accessory box within the Sensor box.
9. Verify you have received all parts. These parts are listed on the packing list and in *Contents of the box* section.
10. Remove the Slide Rail Kit.
11. Pull out the packing material surrounding the Sensor.
12. Remove the Sensor from the antistatic bag.
13. Save the box and packing materials for later use in case you need to move or ship the Sensor.

:

## Setting up the Sensor

This chapter describes how to set up the Sensor for you to configure it.

:

### Setup overview

Setting up a Sensor involves these steps:

1. Position the Sensor.
2. Install interface modules (SFP, SFP+ and QSFP+).
3. Attach power, network, and monitoring cables.
4. Turn on the Sensor.
5. Configure the Sensor after you have set up and turned it on.

:

### How to position the Sensor

Place the Sensor in a physically secure location, close to the switches or routers it will be monitoring. Ideally, the Sensor should be located within a standard communications rack. To mount the Sensor on a rack, you will attach two mounting rails to the Sensor as described in the subsequent sections of this guide.

:

### Install the slide rails and rack mount the Sensor

Trellix recommends rack-mounting your Sensor. For maintenance purposes, you must have access to the front and rear of the Sensor.



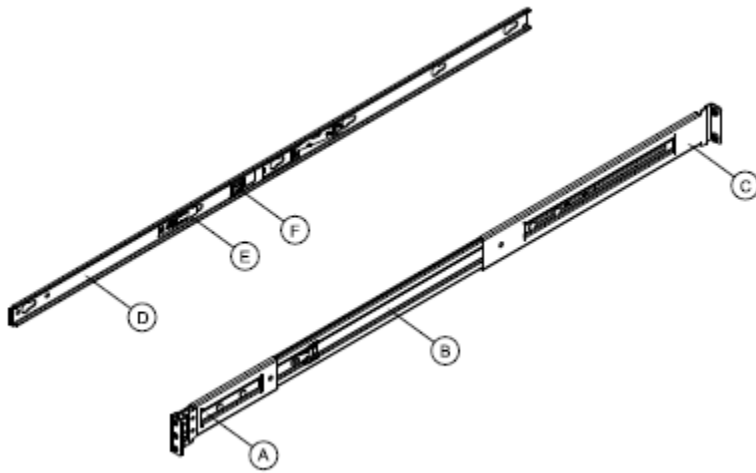
**Caution**

Before you mount the Sensor on the rack, make sure that the power is off. Remove the power cable and all network interface cables from the Sensor.

**Note**

Due to the weight of the appliance, Trellix recommends that two people place the chassis into the rail cabinet.

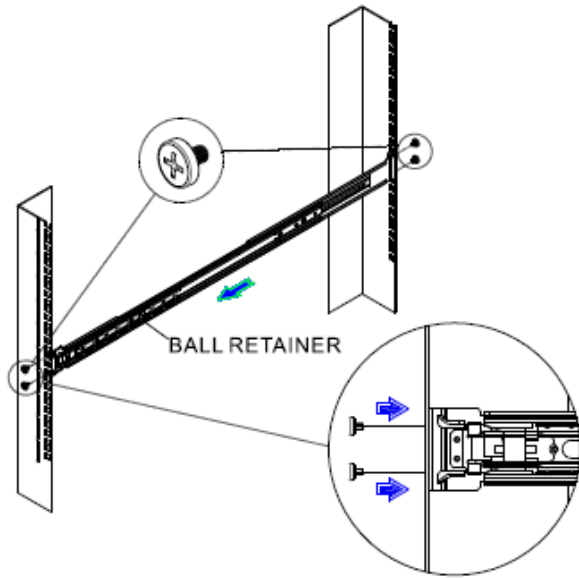
1. Pull the release button to remove inner member from slides.



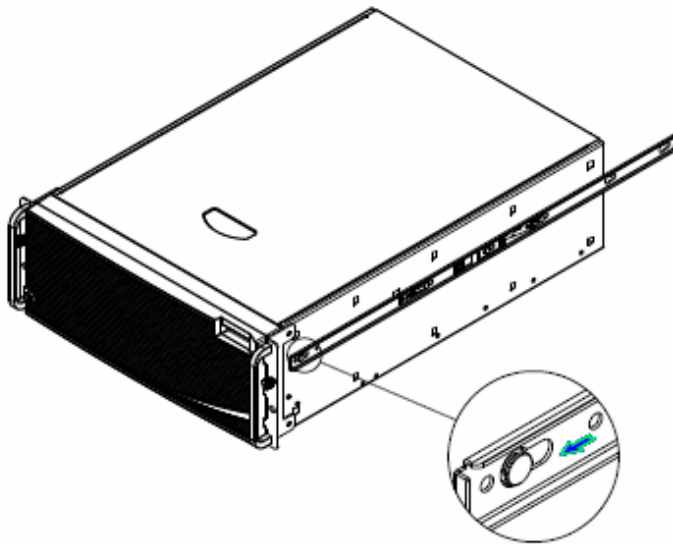
Slides components:

- A - front bracket
- B - outer member
- C - rear bracket
- D - inner member
- E - safety locking pin
- F - release button

2. Align the brackets to appropriate vertical position on the rack and insert the fasteners. Move the ball retainer to the front of the slides.

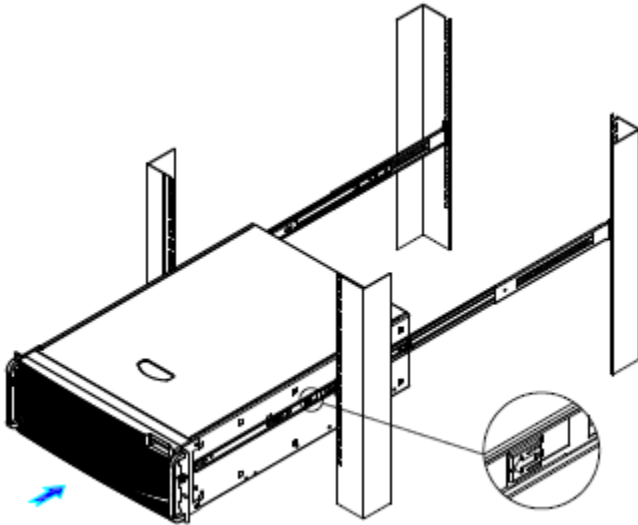


3. Align the inner member key holes to the standoffs on the chassis, then move the inner member toward the front of the

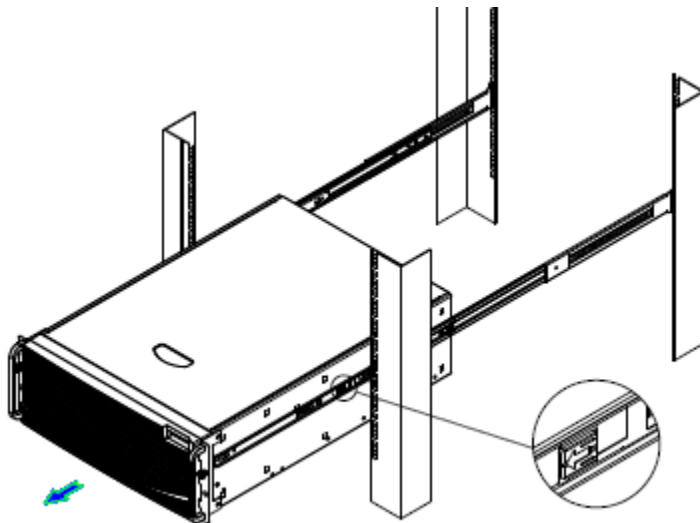


chassis.

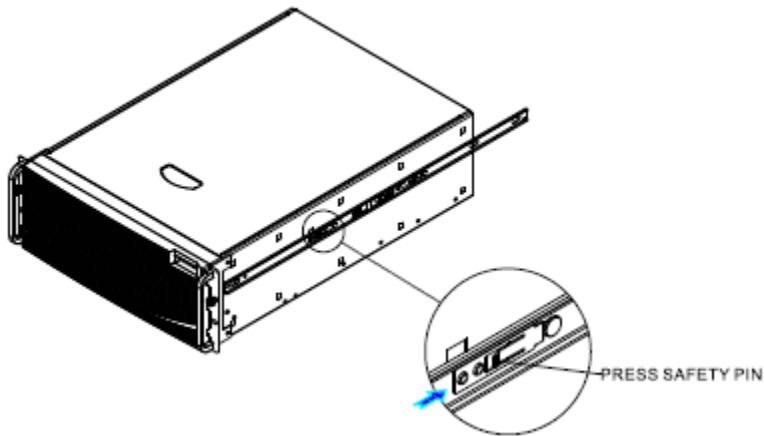
4. Pull the release button on the inner member to release the lock and allow the chassis to close.



5. Install a Sensor into the rack. Optionally, you can also mid-mount the Sensor.
6. Fully extend the slides until it is in the locked position, then pull the release button to release the lock and disconnect the inner member from the slides.



7. Press the safety locking pin to release the inner member from the chassis.



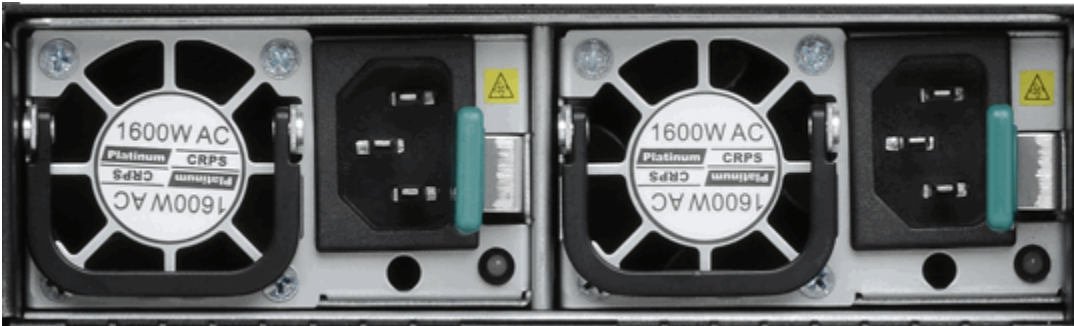
:

## Redundant power supply

The basic configuration of a Sensor includes two hot-swappable power supplies. Each of these modules has one handle for insertion or extraction from the unit as well as a release latch. If you have purchased an additional power supply from Trellix, refer to the following sections to remove and install the new power supply.

---

### Power supply units



:

## Install a new power supply

1. Unpack the power supply from its shipping carton.
2. Remove the faceplate panel covering the power supply slot.

 **Note**

The faceplate panel must remain in place unless a power supply is in the power supply slot. Do not operate the Sensor without the faceplate panel in place.

3. Place the power supply in the slot with the cable outlet facing front and on the left side of the faceplate.
4. Slide in the power supply until it makes contact with the backplane, then push firmly to mate the connectors solidly with the backplane.

 **Note**

For true redundant operation with the power supply, Trellix recommends that you plug each supply into a different power circuit. For optimal protection, use uninterruptable power sources.

:

## Remove the power supply

Perform this task if you want to remove the power supply to the Sensor.

### Steps:

1. Unplug the power cable from its power source and remove the power cable from the power supply.
2. Push the release latch sideways toward the handle.
3. Center the handle of the power supply and pull on it to remove the power supply.
4. Use faceplate panels to protect unused slots from dust and to reduce electromagnetic radiation.
5. Replace the mounting bracket.

 **Caution**

To avoid data interruption, do not turn off both power supplies on an in-line Sensor; or else the Sensor shuts down and all Sensor function stops. Turn off only the power supply that you are replacing.

 **Note**

To remove all power from the Sensor, unplug all power cords.

:

## NS-series Network Interface modules

The NS9x00 Sensors support the 4-port, 6-port, and 8-port Network Interface Modules. These modules need to be installed in the respective slots on the Sensor.

For more information, refer to the *NS-series Interface Modules* section in *Trellix Intrusion Prevention System NS-series Reference Guide*.

:

## Installation of the interface module

This section provides instructions on how to install the interface module based on the following scenarios:

- Install the interface module during a fresh installation of the Sensor.
- Install the interface module on an up and running Sensor.

:

### Install the interface module during a fresh installation of the Sensor

This section provides the steps to install the interface module for a fresh installation of Manager and Sensor.

1. Remove the module from its protective packaging.

#### Note

It is assumed that the Sensor is yet to be powered on, and trust between the Sensor and the Manager has not been established.

2. Grip the sides of the module with your thumb and forefinger and insert the module into the slot.

---

Install an interface module



3. Drive in the screws fixed on the sides of the module to attach it to the Sensor.
4. Turn on the Sensor.
5. Establish trust between the Sensor and the Manager.

:

## Install the interface module on an up and running Sensor

This section provides the steps to install the interface module on a Sensor which is up and running.

### Steps:

1. Power on the Sensor without inserting the pluggable module(s) into the slot(s).
2. Establish trust between the Sensor and the Manager.
3. Grip the sides of the module with your thumb and forefinger and insert the module into the slot.
4. Wait for 5 minutes.
5. Reboot the Sensor from the CLI.

:

## Remove an interface module

Perform these steps if you need to remove an interface module.

1. Disconnect the network fiber optic cable from the module.
2. Remove the transceivers from the module.
3. Unscrew the interface modules to detach them from the Sensor.
4. Place the module into its protective packaging.

:

## Small form-factor pluggable transceiver modules

The NS-series Sensors use three types of small form-factor pluggable transceiver modules as shown in the following table. For more information, see the *NS-series Transceiver Modules* section in *Trellix Intrusion Prevention System NS-series Reference Guide*.

Type	Performance
SFP	1 Gbps (copper) 1 Gbps (fiber optic)
SFP+	1 Gbps (fiber optic) 10 Gbps (fiber optic)
QSFP+	40 Gbps (fiber optic)

Each module is an input/output device that plugs into an LC-type Gigabit Ethernet port, linking the module port with a copper or fiber-optic network. SFP optical interfaces are less than half the size of GBIC interfaces.

To ensure compatibility, Trellix supports only those SFP, SFP+ and QSFP+ modules purchased through Trellix or from a Trellix-approved vendor. For a list of approved vendors, locate the relevant KnowledgeBase article at <https://supportm.trellix.com>. Click Search the Support Knowledge Center.

These installation instructions provide information for installing SFP, SFP+ and QSFP+ modules that use a bail clasp for securing the module in place in the Sensor. Your module might be slightly different. Check the module manufacturer's installation instructions for more details. For ease of installation, insert the module in the Sensor while it is turned off and before placing it on a rack.

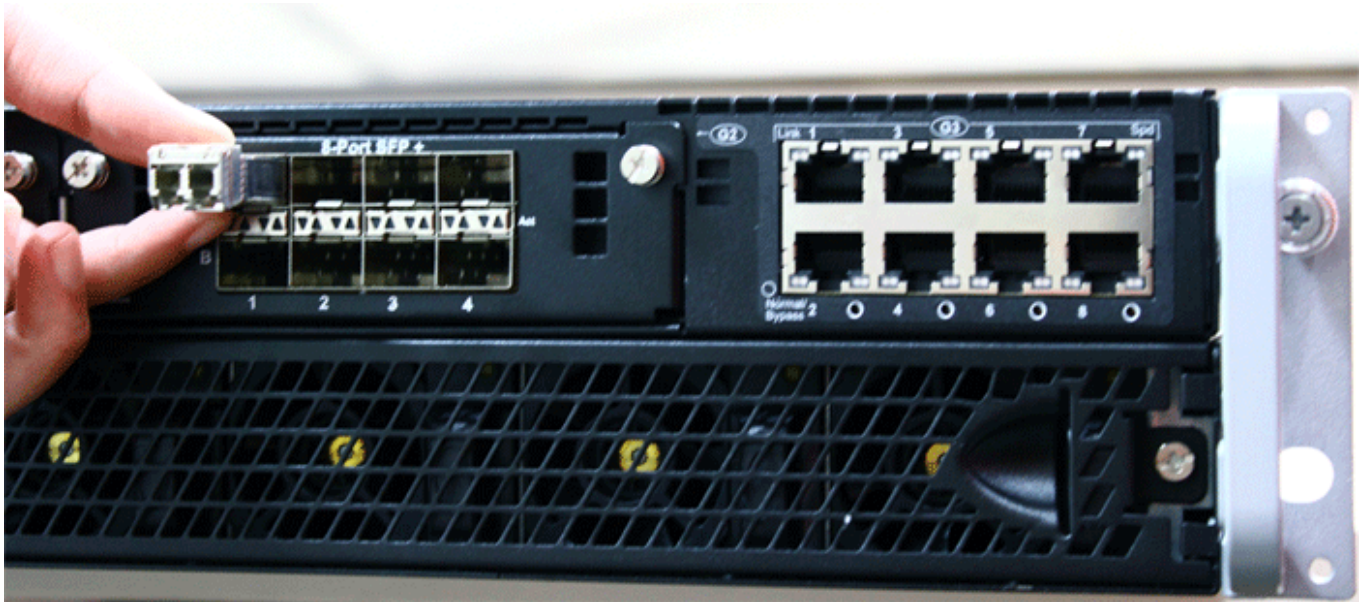
**Caution**

To prevent eye damage, do not stare into open laser apertures.

**Install a transceiver module**

1. Remove the module from its protective packaging.
2. Locate the label on the module and make sure that the alignment groove is down.
3. Grip the sides of the module with your thumb and forefinger and insert the module into the module socket. Modules are keyed to prevent incorrect insertion.

Insert a transceiver module





## Remove a transceiver module

Perform these tasks if you need to remove a module.

### Steps:

1. Disconnect the network fiber-optic cable from the module.
2. Release the module from the slot by pulling the bail clasp out of its locked position.
3. Slide the module out of the slot.
4. Insert the module plug into the module optical bore for protection.

:

## Attaching cables to the Sensor

Follow the steps outlined in this chapter to connect the cables to the various ports of your Sensor.

:

## Connect the cable to the Console port

The Console port on the NS-series Sensor is used for setup and configuration of the Sensor.

### Steps:

1. For console connections, plug the DB9 Console cable supplied by Trellix into the Console port on the Sensor. This port is labeled **Console** in the Sensor front panel.
2. Connect the other end of the Console port cable directly to a COM port of the computer or terminal server you will use to configure the Sensor, for example, a computer 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. Required settings for HyperTerminal are listed below:

Name	Setting
Baud rate	115200
Number of bits	8
Parity	None
Stop bits	1
Flow control	None

3. Turn on the Sensor.

:

### Connect the cable to the Auxiliary port

You can use the Auxiliary port as well for modem access to the Sensor for setup and configuration. You cannot use a modem the first time you configure a Sensor.

1. For modem connections, plug a straight-through modem cable into the Auxiliary port on the NS-series Sensor. This port is labeled **Aux** in the Sensor rear panel.
2. Connect a modem to the **Aux** port.
3. Connect a telephone line to the modem. Required settings for the **Aux** port are given below:

Name	Setting
Baud rate	115200
Number of bits	8
Parity	None
Stop bits	1
Flow control	None

:

### Connect the cable to the Response port

When operating in tap or SPAN mode, the Sensor uses its Response port to respond to attacks. When deployed in tap mode, the Sensor does not inject response packets through the tap but uses the Response port.

1. Plug a Cat-5e Ethernet cable into the Response port. This port is labeled **R1** on the Sensor rear panel.
2. Connect the other end of the cable to the network device such as a hub, switch, or a router, through which you want to respond to attacks.

:

### Connect the cable to the Management port

The Sensor communicates with the Manager using the Management port.

1. Plug a Category 5e Ethernet cable into the Management port. This port is labeled **Mgmt** in the rear panel of the NS-series Sensor.
2. Plug the other end of the cable into the network device connected to your Manager server.

### Note

To isolate and protect your management traffic, Trellix strongly recommends you to use a separate, dedicated management subnet to interconnect the Sensors and the Manager.

:

## Connect the cables to the Interconnect ports

Communication between the NS9300P and NS9300S occurs over the Interconnect ports.

### Steps:

1. Plug the supplied 40G Direct Attach cable into port G0/1 of the NS9300P Sensor and connect the other end of the cable into port G4/1 of the NS9300S Sensor.
2. Plug the supplied 40G Direct Attach cable into port G0/2 of the NS9300P Sensor and connect the other end of the cable into port G4/2 of the NS9300S Sensor.
3. Plug the supplied cable into the Response port (R1) of NS9300P Sensor and connect the other end of the cable into the Management port (Mgmt) port of the NS9300S Sensor.

:

## About connecting cables to the Monitoring ports

Connect to the network devices that you want to monitor through the Sensor monitoring ports. You can deploy Sensors in the following operating modes:

- In-line mode (fail-close)
- In-line mode (fail-open)
- External tap mode
- SPAN or hub mode

:

## How to use peer ports

You must use two peer Monitoring ports of the Sensor to deploy it full duplex mode. On the Sensor, the numbered ports are wired in pairs to accommodate the traffic.

The following Ethernet ports are coupled and must be used together.

 **Note**

- On NS9100, NS9200 and NS9300P Sensors, G0 and G3 indicate the fixed port slots. G1 and G2 indicate the slots for interface modules.
- On NS9300S Sensors, G4 and G7 indicate the fixed port slots. G5 and G6 indicate the slots for interface modules.
- In the following table, it is assumed that G1 is the 2-port QSFP+ 40G interface module, G2 is the 8-Port SFP+/SFP 1/10G interface module, G5 is the 4-port QSFP+ 40G interface module and G6 is the 6-port RJ-45 1 Gbps/100 Mbps/10 Mbps interface module. These interface modules can be interchanged.
- Since monitoring ports are internally wired, the corresponding port is also disabled when you disable one of the ports in a pair.

Port Pairs	Sensor
G0/1 and G0/2	NS9100/NS9200/NS9300P
G1/1 and G1/2	NS9100/NS9200/NS9300P
G2/1 and G2/2	NS9100/NS9200/NS9300P
G2/3 and G2/4	NS9100/NS9200/NS9300P
G2/5 and G2/6	NS9100/NS9200/NS9300P
G2/7 and G2/8	NS9100/NS9200/NS9300P
G3/1 and G3/2	NS9100/NS9200/NS9300P
G3/3 and G3/4	NS9100/NS9200/NS9300P
G3/5 and G3/6	NS9100/NS9200/NS9300P
G3/7 and G3/8	NS9100/NS9200/NS9300P
G4/1 and G4/2	NS9300S
G5/1 and G5/2	NS9300S
G5/3 and G5/4	NS9300S

Port Pairs	Sensor
G6/1 and G6/2	NS9300S
G6/3 and G6/4	NS9300S
G6/5 and G6/6	NS9300S
G7/1 and G7/2	NS9300S
G7/3 and G7/4	NS9300S
G7/5 and G7/6	NS9300S
G7/7 and G7/8	NS9300S

:

## Cable types for routers, switches, hubs and computers

This section lists the types of cables that you require to connect the Sensor to other network devices:

- Use a crossover Ethernet RJ-45 cable to connect a router port to the SFP/SFP+/QSFP+ monitoring ports.
- Use a straight-through Ethernet RJ-45 cable to connect a switch or a hub port to SFP/SFP+/QSFP+ monitoring ports.
- Use a crossover Ethernet RJ-45 cable to connect a router port to computer to the Sensor Management port.
- Use a crossover Ethernet RJ-45 cable to connect a computer to the Sensor monitoring port.

:

## Connect the cables for in-line mode

In-line Gigabit Ethernet ports can be configured as fail-open or fail-close. The RJ-45 monitoring ports are built-in and include an built-in fail-open functionality as well.

All other monitoring ports require the use of external active fail-open (AFO) kits for In-Line Fail-Open Active configuration.

Gigabit Ethernet ports fail-close, means the flow of traffic will stop if the Sensor fails. To allow traffic to flow uninterrupted, you must use special hardware, and cable the Sensor to external active fail-open kits. For instructions, see the subsequent sections of this chapter.

This section provides the steps to connect the Sensor's Gigabit Ethernet ports so they fail-close.

### Steps:

1. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports, for example G1/1.
2. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports, for example G1/2.
3. 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 switch and the one connected to 2 to the router.

:

## Connect the cables for tap mode

To deploy the Sensor in tap mode, you must use a Sensor's Gigabit Ethernet Monitoring port pair with a third-party external tap.

### Note

For a list of Trellix-approved third party vendors, see the KnowledgeBase at <https://supportm.trellix.com>. Enter the relevant KnowledgeBase article in Search the Support Knowledge Center and click Search to locate the relevant KnowledgeBase article.

### Steps:

1. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports, for example, G1/1.
2. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports labeled G1/2.
3. Connect the other end of each cable to the tap.
4. Connect the network devices that you want to monitor to the tap.

:

## Port Clustering for an NS9300 Sensor in tap mode

To improve the attack detection, the traffic distribution between the monitoring ports is redesigned. The monitoring ports are paired such that the traffic from the odd port pairs (G1/1, G1/2) and (G1/5, G1/6) is directed to the local front end of the Sensor, and the traffic from the even port pairs (G1/3, G1/4) and (G1/7, G1/8) is directed to the remote front end of the Sensor. Port cluster in tap mode is configured in a manner where the traffic is being forwarded to the same front end of the Sensor. Port clustering is applicable to ports G1, G2, G3, G5, G6, and G7. Ports G0 and G4 are used as interconnect ports for communication between the primary and secondary Sensors.

The following modules are used for port clustering in an NS9300 Sensor:

- Fixed Gigabit Ethernet-Copper Ports
- Network I/O Modules
  - 8 port (SFP+/SFP) 10/1 GigE
  - 6 port RJ-45 10/100/1000 Mbps

- 4 port (QSFP+) 40 GigE
- 4 port (QSFP+) 10 GigE

### Examples

An 8 -Port 10GigE network interface module consists of 2 odd port pairs and 2 even port pairs:

- Ports 1 and 2 are considered as an odd port pair 1
- Ports 3 and 4 are considered as an even port pair 2
- Ports 5 and 6 are considered as an odd port pair 3
- Ports 7 and 8 are considered as an even port pair 4

**Scenario 1:** If the P-Unit (Primary Sensor) of NS9300 Sensor has an 8 port (SFP+/SFP) 10/1 GigE (G1) network interface module and the S-Unit (Secondary Sensor) of NS9300 Sensor has an 8 port (SFP+/SFP) 10/1 GigE (G5) network interface module, the distribution of traffic from a single source (client/ server) should be either sent to the local front end or the remote front-end of the Sensor, such as:

- The traffic from ports (G1/1, G1/2) and (G1/5, G1/6) is directed to the local front end of the primary Sensor.
- The traffic from ports (G1/3, G1/4) and (G1/7, G1/8) is directed to the remote front end of the secondary Sensor.
- The traffic from ports (G5/1, G5/2) and (G5/5, G5/6) is directed to the local front end of the secondary Sensor.
- The traffic from ports (G5/3, G5/4) and (G5/7, G5/8) is directed to the remote front end of the primary Sensor.

**Scenario 2:** If the existing port cluster setup is for two port pairs (G1/1, G1/2) and (G1/3, G1/4), re-configure to use port pairs (G1/1, G1/2) and (G1/5, G1/6) to accommodate the new design.

**Scenario 3:** If the existing port cluster setup is for three port pairs — (G1/1, G1/2), (G1/3, G1/4) from the P-Unit (Primary Sensor) and (G5/1, G5/2) from the S-Unit (Secondary Sensor) — of NS9300 Sensor, reconfigure to use either of the following port pairs to accommodate the new design.

- (G1/1, G1/2) port pair from the current configuration and add two new port pairs (G1/5, G1/6) and (G5/3, G5/4) to ensure traffic distribution happens at the P-Unit (Primary Sensor) of NS9300 Sensor.
- (G1/1, G1/2) port pair from the current configuration and add two new port pairs (G5/3, G5/4) and (G5/7, G5/8) to ensure traffic distribution happens at the P-Unit (Primary Sensor) of NS9300 Sensor.
- (G1/3, G1/4) and (G5/1, G5/2) port pairs from the current configuration and add one new port pair (G1/7, G1/8) to ensure traffic distribution happens at the S-Unit (Secondary Sensor) of NS9300 Sensor.
- (G1/3, G1/4) and (G5/1, G5/2) port pairs from the current configuration and add one new port pair (G5/5, G5/6) to ensure traffic distribution happens at the S-Unit (Secondary Sensor) of NS9300 Sensor.

**Scenario 4:** If the existing port cluster setup is of four port pairs — (G1/1, G1/2) and (G1/3, G1/4) from the P-Unit (Primary Sensor) and port pairs (G5/1, G5/2) and (G5/3, G5/4) from the S-Unit (Secondary Sensor) — of NS9300 Sensor, reconfigure to use either of the following port pairs to accommodate the new design.

- (G1/1, G1/2) and (G5/3, G5/4) port pairs of the current configuration and add two new port pairs (G1/5, G1/6) and (G5/7, G5/8) to ensure traffic distribution happens at the P-Unit (Primary Sensor) of NS9300 Sensor.
- (G1/3, G1/4) and (G5/1, G5/2) port pairs of the current configuration and add two new port pairs (G1/7, G1/8) and (G5/5, G5/6) to ensure traffic distribution happens at the S-Unit (Secondary Sensor) of NS9300 Sensor.

Refer to the following table to accommodate the design change for port clustering in various interface modules in an NS9300 Sensor:

Modules	Odd and Even Port Pairs
8 port (SFP+/SFP) 10/1 GigE	<p><b>Odd port pairs:</b>  <b>G1:</b> (G1/1, G1/2) and (G1/5, G1/6)  <b>G2:</b> (G2/1, G2/2) and (G2/5, G2/6)  <b>G5:</b> (G5/1, G5/2) and (G5/5, G5/6)  <b>G6:</b> (G6/1, G6/2) and (G6/5, G6/6)</p> <p><b>Even port pairs:</b>  <b>G1:</b> (G1/3, G1/4) and (G1/7, G1/8)  <b>G2:</b> (G2/3, G2/4) and (G2/7, G2/8)  <b>G5:</b> (G5/3, G5/4) and (G5/7, G5/8)  <b>G6:</b> (G6/3, G6/4) and (G6/7, G6/8)</p>
6 port RJ-45 10/100/1000 Mbps	<p><b>Odd port pairs:</b>  <b>G1:</b> (G1/1, G1/2) and (G1/5, G1/6)  <b>G2:</b> (G2/1, G2/2) and (G2/5, G2/6)  <b>G5:</b> (G5/1, G5/2) and (G5/5, G5/6)  <b>G6:</b> (G6/1, G6/2) and (G6/5, G6/6)</p> <p><b>Even port pairs:</b>  <b>G1:</b> (G1/3, G1/4)  <b>G2:</b> (G2/3, G2/4)  <b>G5:</b> (G5/3, G5/4)  <b>G6:</b> (G6/3, G6/4)</p>
4 port (QSFP+) 40 GigE	<p><b>Odd port pairs:</b>  <b>G1:</b> (G1/1, G1/2)  <b>G2:</b> (G2/1, G2/2)  <b>G5:</b> (G5/1, G5/2)  <b>G6:</b> (G6/1, G6/2)</p> <p><b>Even port pairs:</b>  <b>G1:</b> (G1/3, G1/4)  <b>G2:</b> (G2/3, G2/4)  <b>G5:</b> (G5/3, G5/4)  <b>G6:</b> (G6/3, G6/4)</p>
Fixed Gigabit Ethernet-Copper Ports	<p><b>Odd port pairs:</b>  <b>G3:</b> (G3/1, G3/2) and (G3/5, G3/6)  <b>G7:</b> (G7/1, G7/2) and (G7/5, G7/6)</p>



Modules	Odd and Even Port Pairs
	<b>Even port pairs:</b> <b>G3:</b> (G3/3, G3/4) and (G3/7, G3/8) <b>G7:</b> (G7/3, G7/4) and (G7/7, G7/8)

:

## Connect the cables for SPAN or hub mode

For the Sensor, monitoring in SPAN or hub mode occurs in in-line fail-open mode. When you monitor in SPAN or hub mode, you use only single ports.

To connect an Sensor to a SPAN port or hub, plug an LC fiber-optic or 45 cable into one of the modules and connect the other end of the cable to the SPAN port or the hub.

:

## Connect the cables for Sensor Fail-Open

The Fail-Open Kits minimize the potential risks of in-line Sensor failure on critical network links. You need to purchase these kits separately. Both copper and optical versions of the kit are available for the one-gigabit ports. The standard Gigabit Fail-Open Kits, 10 Gigabit Fail-Open Kits and 40 Gigabit Fail-open Kits are available for the 1, 10, and 40 gigabit ports respectively.

The Monitoring ports of the Sensors can be fail-close; thus, if the Sensor is deployed in-line fail-close, a hardware failure results in network downtime. Except the built-in RJ-45 ports which come with built-in fail-open functionality, you use the optional external bypass switch provided in an Active Fail-Open Kit for the Monitoring ports to fail-open.

While the Sensor is operating, the Active Fail-Open kit is in-line and routes all traffic directly through the Sensor. When the Sensor fails, the switch automatically shifts to a bypass state; in-line traffic continues to flow through the network link but is no longer routed through the Sensor. After the Sensor resumes normal operation, the switch returns to the "on" state, enabling in-line monitoring once again.

### Caution

Sensor outage breaks the link connecting the devices on either side of the Sensor for a brief moment and requires the renegotiation of the network link between the two peer devices connected to the Sensor. Depending on the network equipment, this disruption introduced by the renegotiation of the link layer between the two peer devices might range from a couple of seconds to more than a minute with certain vendors' devices.

**Caution**

A very brief link disruption might also occur while the links between the Sensor and each of the peer devices are renegotiated to place the Sensor back in in-line mode. This outage, again, varies depending on the device, and can range from a few seconds to more than a minute.

The performance of the switchover from in-line to bypass and vice versa varies depending on the vendor.

You can find the installation and troubleshooting instructions for the kit in the guide that accompanies the kit. For example, for more information on the Optical kits, see the following guides:

- *1 Gigabit Optical Active Fail-Open Bypass Kit Guide*
- *10 Gigabit Optical Active Fail-Open Bypass Kit Guide*
- *40 Gigabit Optical Active Fail-Open Bypass Kit Guide*
- *Active Fail-Open Kit Quick Start Guide*
- *Passive Fail-Open Kit Quick Start Guide*

:

## Connect the cable for Sensor failover

For Sensor failover, connect two NS-series Sensors using the appropriate cables. These two Sensors must be running the same software version. Failover cables are the only additional hardware required to support failover communication between two NS-series Sensors.

Refer to the following table before you configure a failover pair:

Sensor Model	Port to connect the failover pair	Cable requirements for failover
NS9300	G1/1 and G1/2	2 40G QSFP Copper direct connect cable
NS9200	G0/1	1 40G QSFP Copper direct connect cable
NS9100	G0/1	1 40G QSFP Copper direct connect cable

Trellix ships the cable required for failover pair creation, along with the Sensor hardware.

The length of this cable is 3 meters. If you need to configure a failover pair between Sensors kept at distance greater than 3 meters, consider the following options:

- Failover between 3 meters - 100 meters: Purchase fiber Active Optical Cable (AOC) or QSFP+ SR4 transceiver module from Trellix or QSFP+ SR4 transceiver module from an external source.
- Failover between 100 meters - 300 meters: Purchase QSFP+ SR4 transceivers from Trellix or QSFP+ SR4 transceiver from an external source.
- Failover above 300 meters: Purchase QSFP+ LR4 transceivers from Trellix or QSFP+ LR4 transceivers from an external source.

### Steps:

1. Plug the cable(s) appropriate for use with your QSFP+ module into port G0/1 (NS9100, NS9200) or G1/1 and G1/2 (NS9300) of the active NS-series Sensor.
2. Connect the other end of the cable(s) into port G0/1 (NS9100, NS9200) or G1/1 and G1/2 (NS9300) of the standby NS-series Sensor.

:

## Turning the Sensor on and off

### Note

Do not attempt to turn on the Sensor until you have installed the Sensor in a rack and made all the necessary network connections.

### Steps:

1. Connect the power cable to the Sensor power supply.
2. Connect the power cable to a power source.

### Note

If you are installing a redundant power supply, you should install it as described in *Install a new power supply* section. For true redundant operation with the redundant power supply, Trellix recommends that you plug each supply into a different power circuit.

The Sensor has no power switch. The Sensor turns on as soon as one of its power cables is connected to a power source. Trellix recommends that you use the **shutdown** CLI command to halt the Sensor before turning it off. For more information on CLI commands, see the *CLI commands* section in *Trellix Intrusion Prevention System Product Guide* for specific Sensor software version you are running.

:

## Configure the Sensor and Manager for deployment

:

## 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.


### Steps:

1. Prepare the system according to the requirements outlined in *Trellix Intrusion Prevention System Installation Guide*.
2. Close all open applications.
3. Go to [Trellix Download Server \(https://www.trellix.com/en-us/downloads/my-products.html\)](https://www.trellix.com/en-us/downloads/my-products.html).
4. Log on using your **Grant Number** and registered **Email Address**.  
The Find Products page opens.
5. In the Category filter, select Network Security.
6. Click on the Manager version required.  
The Available Downloads page opens.
7. In the Type filter, select Installation.  
The Manager installation files available for download are listed.
8. Click on the required Manager installation file and the download starts.
9. Refer to *Trellix Intrusion Prevention System Installation Guide* for detailed procedure to install the Manager application.

:

## Add the Sensor to the Manager

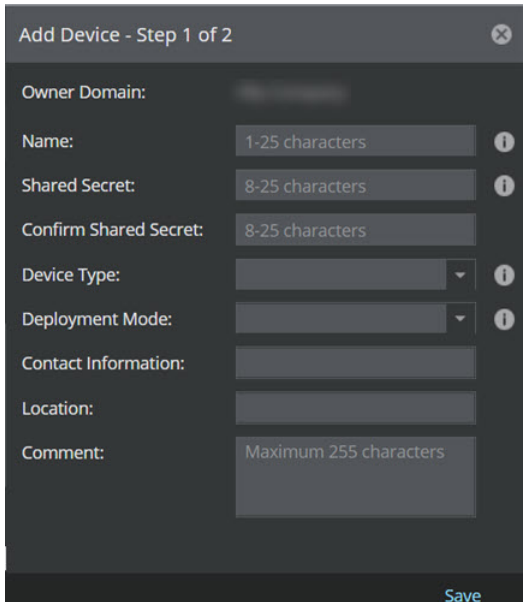
### Steps:

1. Log on to the Manager using the default user name (**admin**) and password (**admin123**).
2. Go to Devices → <Admin Domain Name> → Global → Device Manager.  
The Device Manager page is displayed.
3. 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.



4. Enter the following mandatory information in the appropriate fields:

- Name — The Sensor name must begin with a letter. The maximum length of the name is 25 characters.
- 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 enter later 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.

- Device Type — Specifies the type of device to be added. Select IPS Sensor.
- Deployment Mode — Select Direct or Indirect.

 **Note**

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

- Contact Information — (Optional) Type the contact information.
- Location — (Optional) Type the location.
- Comment — (Optional) Type the comment.

5. Click Save.

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

:

### 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.



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.

Steps:

1. Log on to the Sensor using the terminal connected to the Console port.
2. At the prompt, log on using the default Sensor username (**admin**) and password (**admin123**).

```
login as: admin
* * *

Authorized users only. Unauthorized users will be prosecuted
to the full extent of the law.

* * *
Using keyboard-interactive authentication.
Password:
Last login: Fri Sep 28 07:20:31 2012 from 172.16.230.77
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is 'off'.

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

3. (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.

4. 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.

At the prompt, type: **set sensor name <word>**. 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.

5. 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**
6. 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**
7. 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.

8. If prompted, reboot the Sensor. Type **reboot**

 **Note**

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

9. 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 that the information is correct.

- 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.

- Type **show** to verify the configuration information. Check that all information is correct.
- Type **exit** to exit the session.

:

## Verify successful installation

### Steps:

- Type **status** in the Sensor CLI. The status report appears.

```

intruShell@ns > status
[Sensor]
System Initialized      : yes
System Health Status   : good
Layer 2 Status         : normal (IDS/IPS)
Installation Status    : complete
IPv6 Status            : Dont Parse and Allow Inline
Reboot Status          : Not Required
Guest Portal Status    : up
Hitless Reboot         : Available
Last Reboot reason     : reboot issued from NSM

[Signature Status]
Present                : yes
Version                : 
Power up signature     : good
Geo Location database  : Present
DAT file               : Present
DAT file Version       : 1937.0

[Manager Communications]
Trust Established      : yes (RSA 2048-bit with SHA2 support)
Alert Channel         : up
Log Channel           : up
Authentication Channel : up
Last Error            : None
Alerts Sent           : 344630
Logs Sent             : 208586

[Alerts Detected]
Signature              : 8507889      Alerts Suppressed : 8322935
Scan                   : 3282        Denial of Service : 1113
Malware                 : 0

[MCAfee MATD Communication]
Status                 : down
IP                     : 0.0.0.0
Port(Secure)          : 8505

```

The Sensor parameter **System Initialized** should be **yes**, and for Manager communication **Trust Established** should be **yes**.

- Return to the Manager. In the Manager Home page, view the Manager status in the System Faults section. The Manager status should be up and Sensor status should be active.



System Faults					
Manager	Status	Critical	Error	Warning	
Manager	Up	1	1	0	
Device	Status	Critical	Error	Warning	
Doc_NS-series_Sensor_1	Active	6	0	3	
Doc_NS-series_Sensor_2	Active	4	1	3	
NS9500_Stack-1	Unknown	0	0	0	
NS9500_Stack-2	Unknown	0	0	0	
NSP_Doc_Sensor_1	Active	0	0	0	
NSP_Doc_Sensor_2	Active	1	0	0	
NSP_Doc_VM600_1	Active	0	0	0	
NSP_Doc_VM600_2	Active	0	0	0	

- From the Manager Home page, click Configure to open the Configuration page.
- Select your added Sensor: Device List → <Device\_Name>. The ports for this Sensor appear under the <Device\_Name> node.

### Note

<Device\_Name> indicates the name of the Sensor you added.

/NSP_Doc_03 > Doc_NS-series_Sensor_1 > Setup > Physical Ports					
Physical Ports					
Monitoring Ports		Response Ports	Management Port		
Port	Link	Virtual Adapter	Operation Mode	Placement	Response Port
I/O Module: G0 (2-port Q5FP+ module detected)					
0/1	---	---	---	---	---
0/2	---	---	---	---	---
I/O Module: G1 (empty)					
---	---	---	---	---	---
I/O Module: G2 (empty)					
---	---	---	---	---	---
I/O Module: G3 (8-port RJ-45 module detected)					
3/1	Disabled	In-line Fail Open (Paired with 3/2)	Inside Network	This Port	
3/2	Disabled	In-line Fail Open (Paired with 3/1)	Outside Network	This Port	
3/3	Up	In-line Fail Open (Paired with 3/4)	Inside Network	This Port	
3/4	Up	In-line Fail Open (Paired with 3/3)	Outside Network	This Port	
3/5	Up	In-line Fail Open (Paired with 3/6)	Inside Network	This Port	
3/6	Up	In-line Fail Open (Paired with 3/5)	Outside Network	This Port	
3/7	Disabled	In-line Fail Open (Paired with 3/8)	Inside Network	This Port	
3/8	Disabled	In-line Fail Open (Paired with 3/7)	Outside Network	This Port	

- 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 IPS-provided policies, you can clone the policy and then customize it as described in *Trellix Intrusion Prevention System Product Guide*.

6. Click Device List → <Device\_Name> → Port Settings.
7. 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*.

:

## You're up and running!

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

### Steps:

1. For detailed usage instructions, see *Trellix Intrusion Prevention System Product Guide*, or click the ? buttons in the upper-right corner of each window in the Manager.
2. Start the Analysis → <Admin Domain> → Attack Log to view alert statistics as attacks are detected. A summary of alerts is displayed in the Unacknowledged Alert Summary monitor of the Manager Dashboard page.
3. Having problems? Check *Trellix Intrusion Prevention System Product Guide* for troubleshooting information.
4. 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://supportm.trellix.com>.

:

## Troubleshooting the Sensor

This section lists some common installation problems, the possible causes, and the corresponding solutions.

Problem	Possible Cause	Solution
LED is off.	The Sensor is turned off.	Restore Sensor power.

<b>Problem</b>	<b>Possible Cause</b>	<b>Solution</b>
LED is off.	The Sensor port cable is disconnected.	Check the Sensor cable connections.
Sensor is operational but is not monitoring traffic.	Network device cables have been disconnected.	Check the cables and make sure they are properly connected to both the network devices and the bypass switch.
Sensor is operational but is not monitoring traffic.	The Sensor ports have not been enabled in the Manager.	The Sensor will not monitor traffic on the ports unless the ports are enabled in the Manager. Ports are disabled in case of Sensor failure; you must re-enable them for Sensor monitoring to resume.
Network or link problems	Improper cabling or port configuration	Make sure that the transmitting and receiving cables are properly connected to the bypass switch.
Runts or giants errors on switch and routers	Improper cabling or port configuration	Make sure that the transmitting and receiving cables are properly connected to the bypass switch.
The system fault "Switch absent" appears in the Manager Status page.	The Active Fail-Open Kit is disconnected.	Check the Active Fail-Open Kit and make sure it is properly connected to the Sensor.

:

## Sensor technical specifications

The following table lists the specifications of for NS9x00 Sensors.

Sensor Specifics	NS9100	NS9200	NS9300
Dimensions	2RU Rack Mountable 17.24" (W) x 3.44" (H) x 28.76" (D)	2RU Rack Mountable 17.24" (W) x 3.44" (H) x 28.76" (D)	2 x 2RU Rack Mountable 17.24" (W) x 6.88" (H) x 28.76" (D)
Weight	67 lbs.	67 lbs.	134 lbs.
Storage	Dual Solid State 300 GB in RAID 1 configuration	Dual Solid State 300 GB in RAID 1 configuration	600 GB (2 x Dual Solid State 300 GB in RAID 1 configuration)
<b>System Heat Dissipation</b>			
Maximum BTU	4191 BTU/hr	4191 BTU/hr	8382 BTU/hr
Typical BTU	3338 BTU/hr	3709 BTU/hr	7417 BTU/hr
Maximum Power Consumption	1130w	1130w	2260w
Redundant Power Supply	Included	Included	Included
Power	100-240 VAC (50/60Hz)		
Temperature	0° - 35° C (operating) -40° - 70° C (non-operating)		
Relative humidity (non-condensing)	Operational: 10% - 90% Non-operational: 5% - 95%		
Altitude	0 to 10,000 feet		
Safety Certification	UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB license and report covering all national country deviations.		
EMI Certification	FCC Part 15, Class A (CFR 47) (USA) ICES-003 Class A (Canada), EN55022 Class A (Europe), CISPR22 Class A (Int'l)		

:

# NS7500 Sensor

:

## About Sensors

Sensors are high-performance, scalable, and flexible content processing appliances built for the accurate detection and prevention of:

- Network intrusions
- Network misuse
- Distributed Denial-of-Service (DDoS) attacks

Sensors are specifically designed to handle traffic at wire speed, efficiently inspect and detect intrusions with a high degree of accuracy, and flexible enough to adapt to the security needs of any enterprise environment. When deployed at key network access points, the Sensor provides real-time traffic monitoring to detect malicious activity and respond to the malicious activity as configured by the administrator.

After you deploy a Sensor successfully, you configure and manage it using the Manager. The process of configuring a Sensor and establishing communication with the Manager is described in subsequent chapters of this guide. For the details about the Manager, see the *Manager Administration* section in *Trellix Intrusion Prevention System Product Guide*.

:

## Functions of an NS-series Sensor

The NS-series Sensors are a third-generation hardware platform for Sensors designed for high bandwidth links to offer Next Generation IPS (NGIPS) capability and provide high aggregate throughput across various Sensor models. The NS7500 Sensor is a 1RU unit providing an aggregate throughput of 3 Gbps, 5 Gbps, and 7.5 Gbps.

The primary function of a Sensor is to analyze traffic on selected network segments and to respond when an attack is detected. The Sensor examines the header and data portion of every network packet, looking for patterns and behavior in the network traffic that indicate malicious activity. The Sensor examines packets according to user-configured policies, or rule sets, which determine what attacks to watch for, and how to respond with countermeasures if an attack is detected.

If an attack is detected, a Sensor responds according to its configured policy. Sensor can perform many types of attack responses, including generating alerts and packet logs, resetting TCP connections, "scrubbing" malicious packets, and even blocking attack packets entirely before they reach the intended target.

:

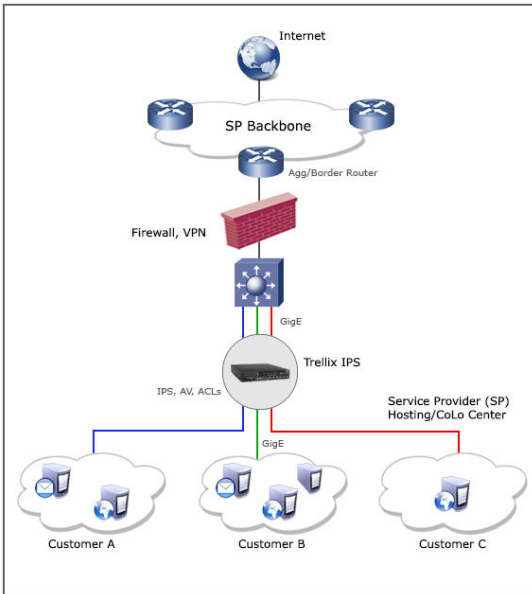
## Deployment of an NS-series Sensor

Deployment of a Sensor requires knowledge of your network to help determine the level of configuration and the number of installed Sensors. You also need to determine the number of Trellix ePolicy Orchestrator - On-prem servers required to protect your network. The Sensor is purpose-built for the monitoring of traffic across one or more network segments.

Following is an example of a network topology using Gigabit Ethernet throughput. In the illustration, Trellix Intrusion Prevention System provides IPS protection to outsourced servers. High port-density and virtualization provides a highly scalable solution, while Trellix IPS protects against web and eCommerce mail server exploits.

---

### A sample NS-Series Sensor deployment



:

## NS-series physical description

The high-port density NS-series Sensor is designed for high bandwidth links. The NS7500 Sensor operates at 3 Gbps, 5 Gbps, or 7.5 Gbps throughput depending on the license purchased. This section gives a physical description of the NS-series Sensor.

:

### Components of an NS-series Sensor

Correlate the pictures with the information following it to understand the components of an NS-series Sensor.

---

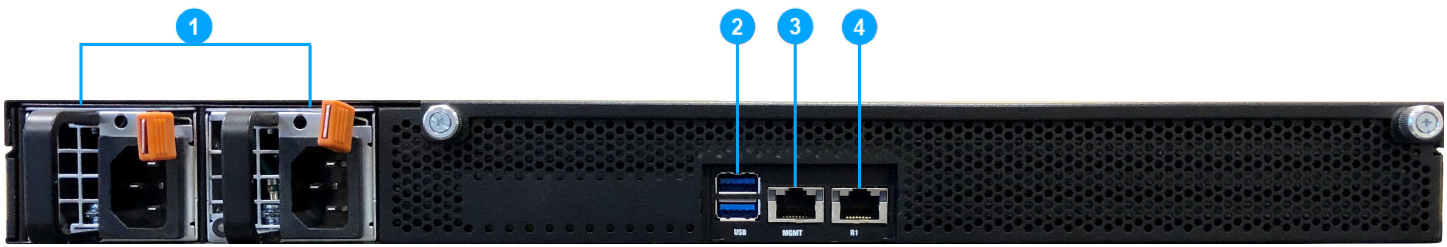
#### Sensor front panel



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.

#### 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)

:

### Sensor LEDs

The front and rear panel LEDs provide status information for the health of the Sensor and the activity on its ports. The following table describes the NS-series LEDs.



## Front panel LEDs

LED	Status	Description
Status	Green Amber	Sensor is operating in good health. Sensor is booting up. It also indicates system bad health if the LED is on for longer duration
Fan	Green Amber	All five fans are operating. One or more fans are not working.
Temp	Green Amber	Inlet air temperature measured inside the chassis is normal. (Chassis temperature OK) Inlet air temperature measured inside the chassis is too high. (Chassis temperature too hot)
Gigabit Ports Speed	Green Amber Off	The port speed is 1000 Mbps. The port speed is 100 Mbps. The port speed is 10 Mbps.
4-port RJ-45 I/O module	Green Amber Off	The port speed is 10000 Mbps. The port speed is 1000 Mbps. The port speed is 100 Mbps.
Gigabit Ports Link	Green Off	The link is up . The link is down.
RJ-45 Fail Open/Bypass	Green Off	The port pair is in Inline Fail-Open/Inline Fail-Close/SPAN/Tap Mode. The Port Pair is in the Bypass Mode.

## Rear panel LEDs

LED	Status	Description
Pwr A (Power A)	Solid Green Blinking Green Solid Amber	Power Supply A is functioning. Power Supply A is stand-by. Power Supply A is not functioning or the unit has no power feed.
Pwr B (Power B)	Solid Green Blinking Green Solid Amber	Power Supply B is functioning. Power Supply B is stand-by. Power Supply B is not functioning or the unit has no power feed.
Management Port Speed	Green Amber Off	The port speed is 10000 Mbps. The port speed is 1000 Mbps. The link is down.
Management Port Link/Act	Green Blinking Green Off	The link is up. Data is received or transmitted. The link is down.
Response Port Speed	Green Amber Off	The port speed is 10000 Mbps. The port speed is 1000 Mbps. The link is down.
Response Port Link/Act	Green Blinking Green Off	The link is up. Data is received or transmitted. The link is down.

:

## Before you install

This chapter describes the best practices for deployment of Sensors in your network. Topics include the safety considerations for handling the Sensor, usage restrictions that apply to the Sensor model, and the contents that are shipped along with the Sensor.

:

## Usage restrictions

The following restrictions apply to the use and operation of a Sensor:

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

:

## Safety measures

Please read the following warnings before you install the Sensor. These safety measures apply to all Sensor models unless otherwise noted. Failure to observe these safety warnings could result in serious physical injury.

### Warnings:

- Read the installation instructions before you connect the system to its power source.
- To remove all power from the Sensor, unplug all power cords, including the redundant power cord.
- Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
- Before working on the equipment that is connected to power lines, remove all jewelry including rings, necklaces, and watches. Metal objects will heat up when connected to power and ground, and can cause serious burns or weld the metal object to the terminals.
- This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.
- Do not remove the outer shell of the Sensor. Doing so will invalidate your warranty.
- Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Blank faceplates and cover panels prevent exposure to hazardous voltages and currents inside the chassis, contain electromagnetic interference (EMI) that might disrupt other equipment and direct the flow of cooling air through the chassis.
- To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the users will be required to correct the interference at their own expense.
- Refer to the Appendix for information on regulatory, compliance, and other safety requirements.

:

## About fiber-optic ports

The Sensor uses fiber-optic connectors for its Monitoring ports. The connector type is an SFP/SFP+ fiber optic connector that is LC-duplex compatible.

Note the following:

- Fiber-optic ports (for example, SFP/SFP+, FDDI, OC-3, OC-12, OC-48, ATM, GBIC, and 100BaseFX) are considered Class 1 laser or Class 1 LED ports.
- These products have been tested and found to comply with Class 1 limits of IEC 60825-1, IEC 60825-2, EN 60825-1, EN 60825-2, and 21CFR1040.

### Caution

To avoid exposure to radiation, do not stare into the aperture of a fiber-optic port. Invisible radiation could be emitted from the aperture of the port when no fiber cable is connected.

- Only FDA registered, EN 60825-1 and IEC 60825-1 certified Class 1 SFP/SFP+ laser transceivers are acceptable for use with the Sensor.

:

## Contents of 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)

:

## Unpack the Sensor

Steps:

1. Open the crate.
2. Remove the first accessory box.
3. Verify you have received all parts. These parts are listed on the packing list and in [Contents of the box](#) section.
4. Remove the Sensor.
5. Place the Sensor box as close to the installation site as possible.

6. Position the box with the text upright.
7. Open the top flaps of the box.
8. Remove the accessory box within the Sensor box.
9. Verify you have received all parts. These parts are listed on the packing list and in [Contents of the box](#) section.
10. Remove the Slide Rail Kit.
11. Pull out the packing material surrounding the Sensor.
12. Remove the Sensor from the antistatic bag.
13. Save the box and packing materials for later use in case you need to move or ship the Sensor.

:

## Setting up the Sensor

This chapter describes how to set up the Sensor for you to configure it.

:

### Setup overview

Setting up a Sensor involves these steps:

1. Position the Sensor.
2. Install the supported interface modules as per your requirement.
3. Attach power, network, and monitoring cables.
4. Turn on the Sensor.
5. Configure the Sensor after you have set up and turned it on.

:

### How to position the Sensor

Place the Sensor in a physically secure location, close to the switches or routers it will be monitoring. Ideally, the Sensor should be located within a standard communications rack. To mount the Sensor on a rack, you will attach two mounting rails to the Sensor as described in the subsequent sections of this guide.

:

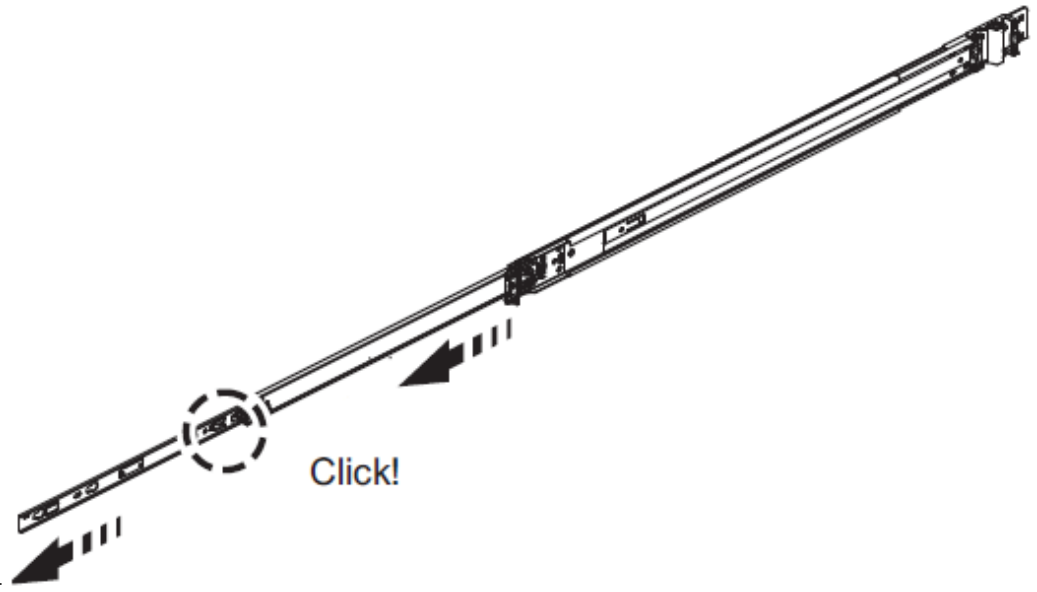
### Install the slide rails and rack mount the Sensor

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

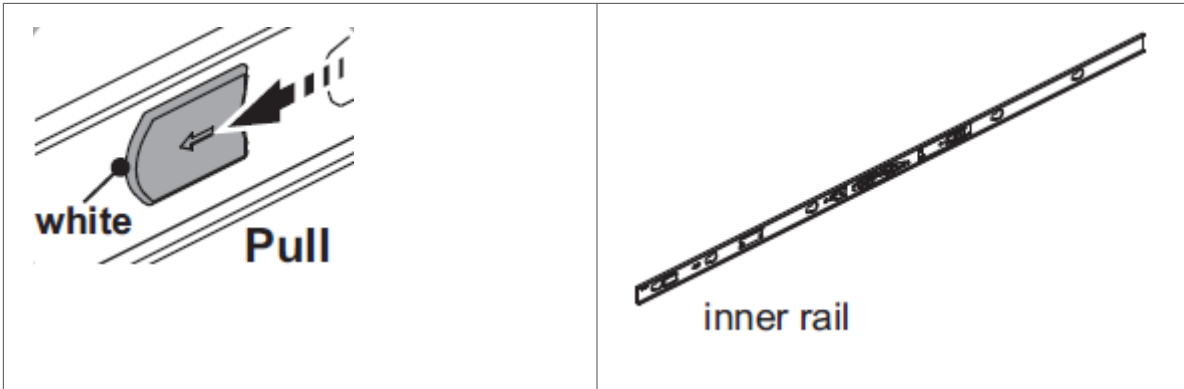
#### Note

Due to the weight of the appliance, Trellix recommends that two people place the chassis into the rail cabinet.

1. Disassemble the inner slide rails from the rail assemblies.

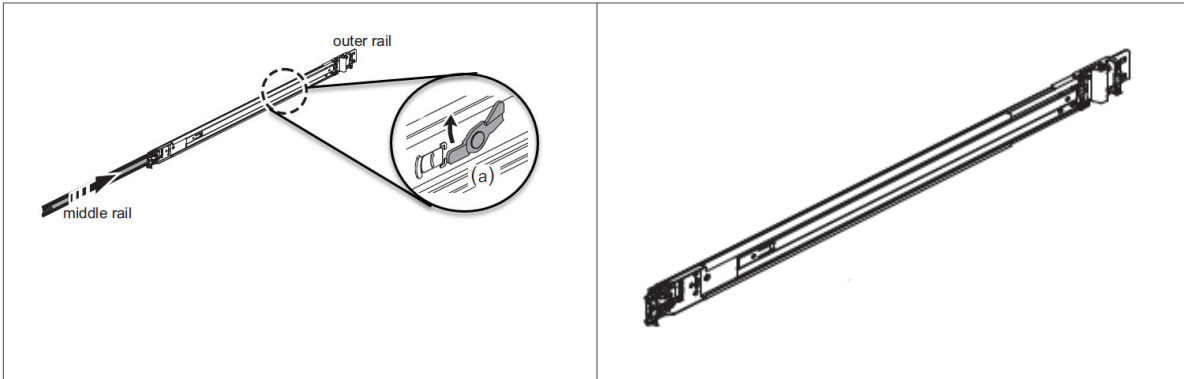


- a. Pull the inner rail out.
- b. Click and pull the white tab (lock on inner rail) forward to disconnect inner rail from the middle rail.



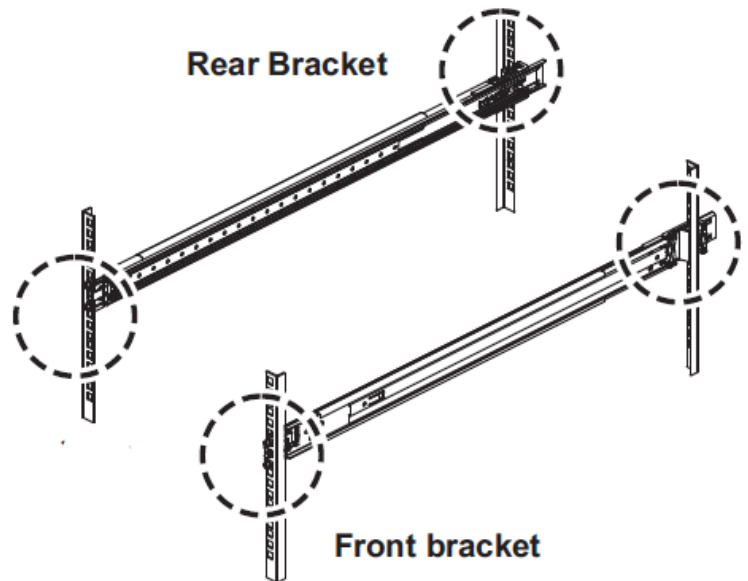
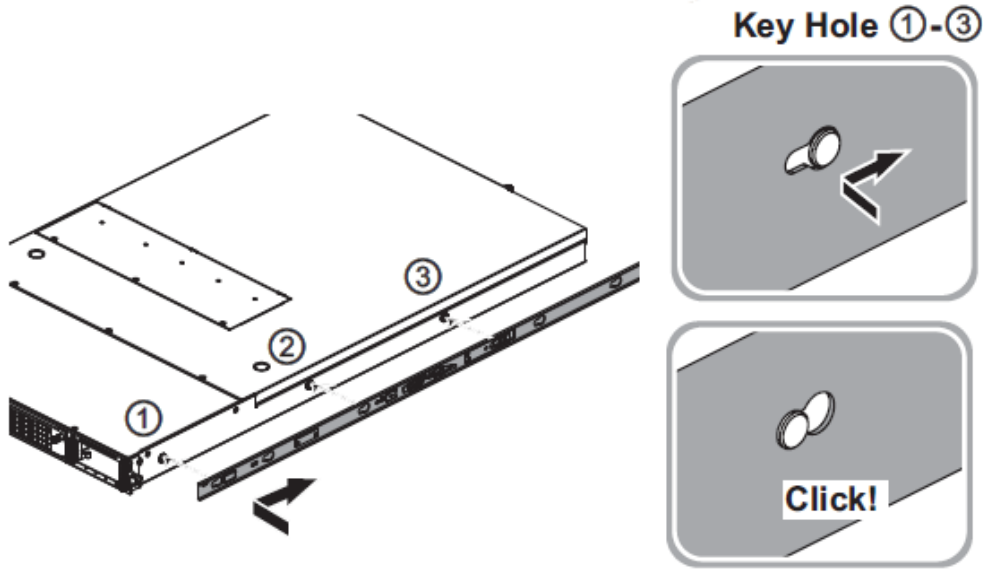
The Inner rail is disconnected.

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



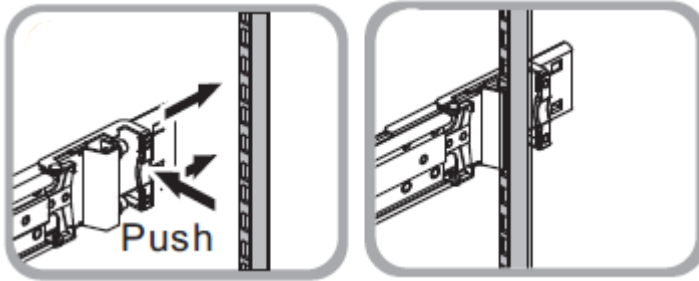
The middle rail is pushed back into the outer rail.

2. 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.



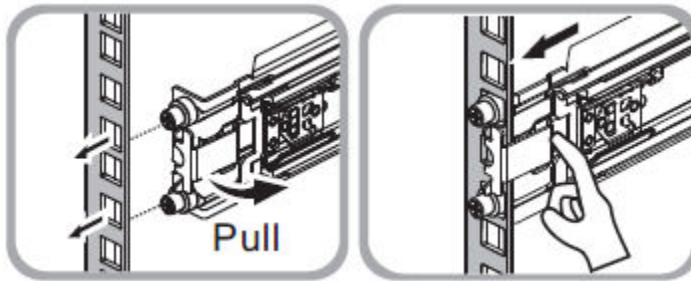
3. Mount the outer slide rails/brackets to the rack posts.

- 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



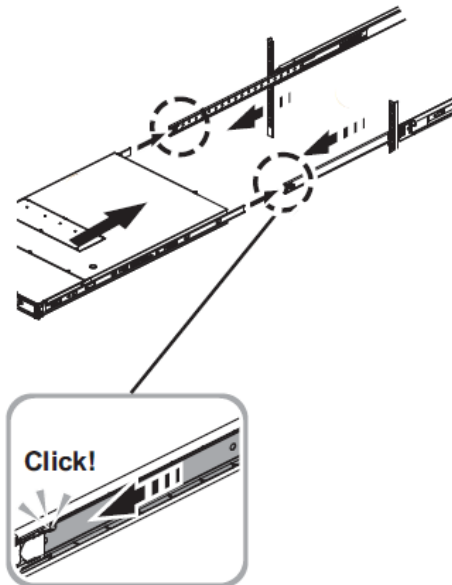
the securing latch onto the rack post.

- 4. Mount the chassis unit into the rack.

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

 **Note**

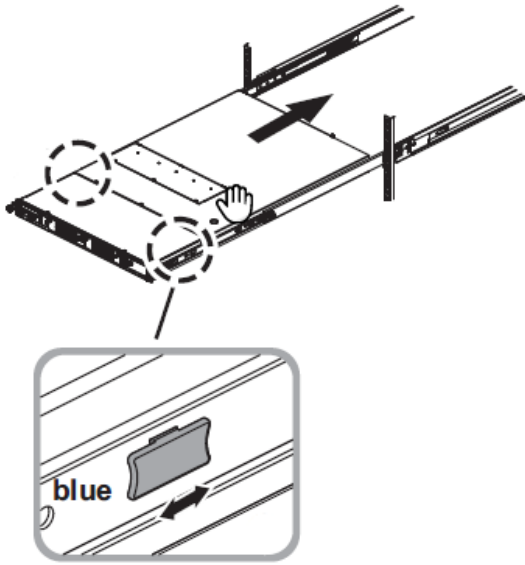
Ensure ball bearing retainer is located at the front of the middle rail.



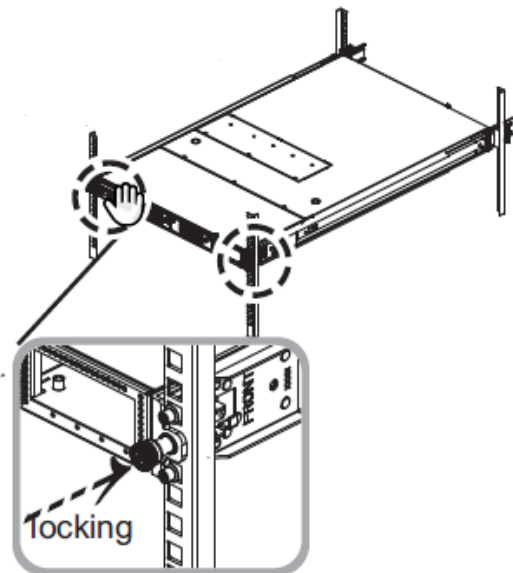
- b. Insert the chassis unit into the middle rails.



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.



## NS-series interface modules

The NS7500 Sensors support the 4-port, 6-port, and 8-port Network Interface Modules. These modules need to be installed in the respective slots on the Sensor.

For more information, refer to the *NS-series Interface Modules* section in *Trellix Intrusion Prevention System NS-series Reference Guide*.

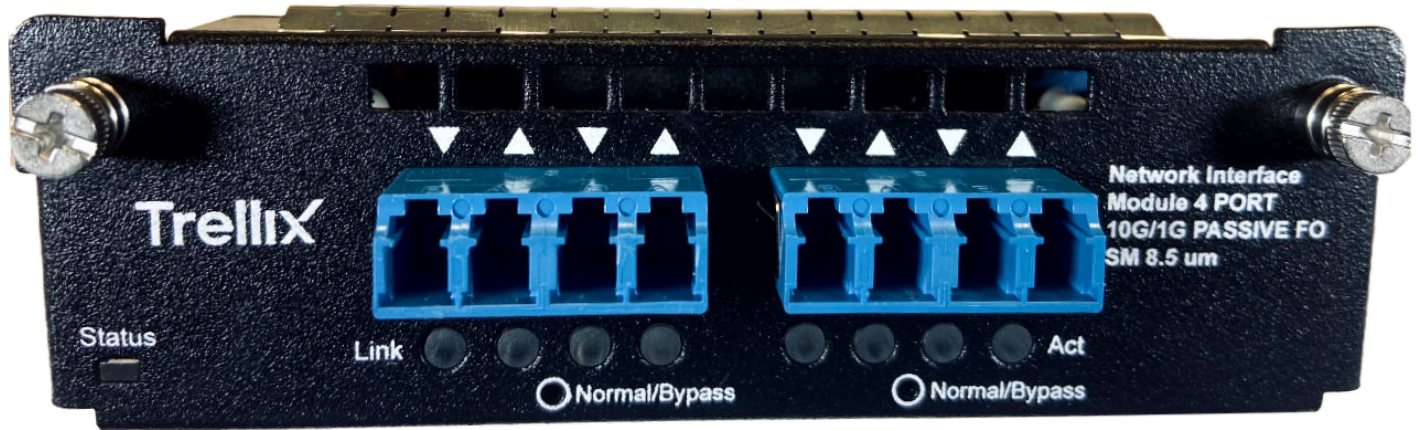
:

### 4-port 10/1 GigE SM 8.5 $\mu\text{m}$ with internal fail-open Network Interface Module

The 4-port SM 8.5  $\mu\text{m}$  Network Interface Module provides internal fail-open capability with 10/1 Gigabit Ethernet performance on each port.

---

4-port 10/1 GigE SM 8.5  $\mu\text{m}$  with internal fail-open interface module



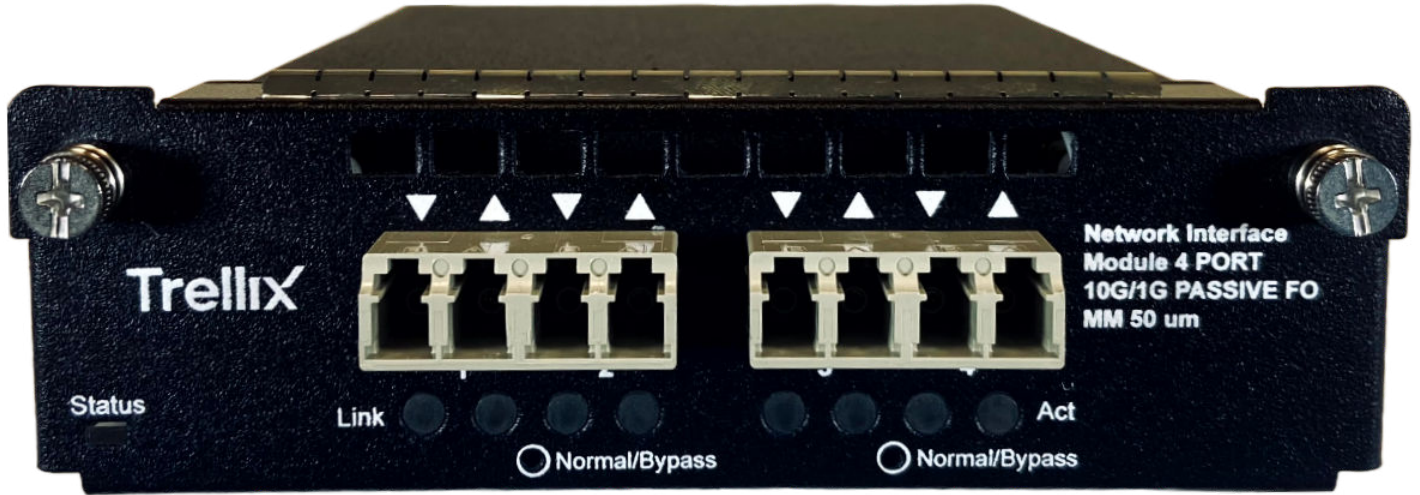
:

### 4-port 10/1 GigE MM 50 $\mu\text{m}$ with internal fail-open Network Interface Module

The 4-port MM 50  $\mu\text{m}$  Network Interface Module provides internal fail-open capability with 10/1 Gigabit Ethernet performance on each port.

---

4-port 10/1 GigE SM 50  $\mu\text{m}$  with internal fail-open interface module

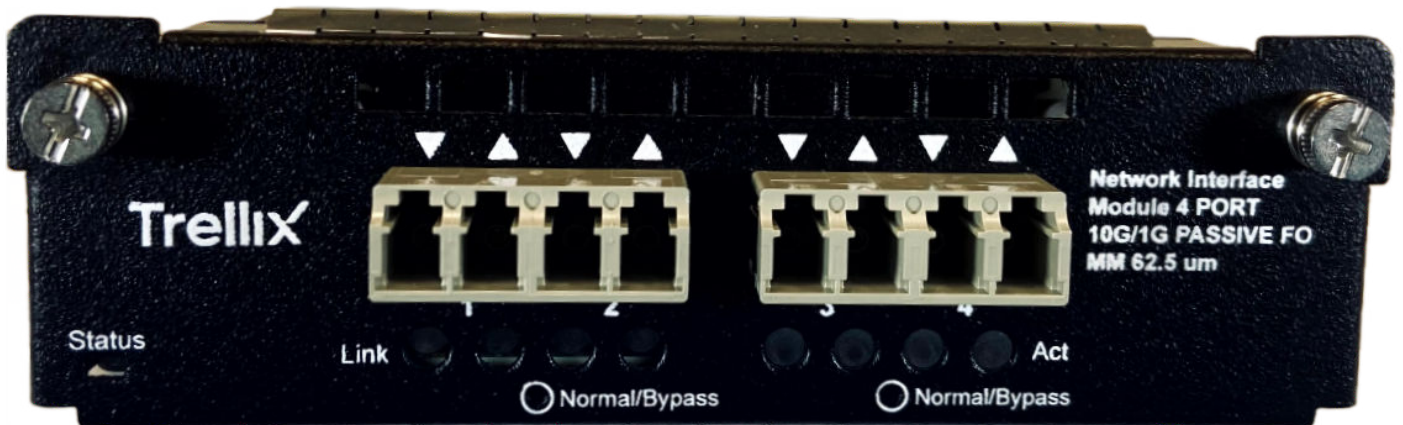


:

### 4-port 10/1 GigE MM 62.5 $\mu$ m with internal fail-open Network Interface Module

The 4-port MM 62.5  $\mu$ m Network Interface Module provides internal fail-open capability with 10/1 Gigabit Ethernet performance on each port.

4-port 10/1 GigE SM 62.5  $\mu$ m with internal fail-open interface module



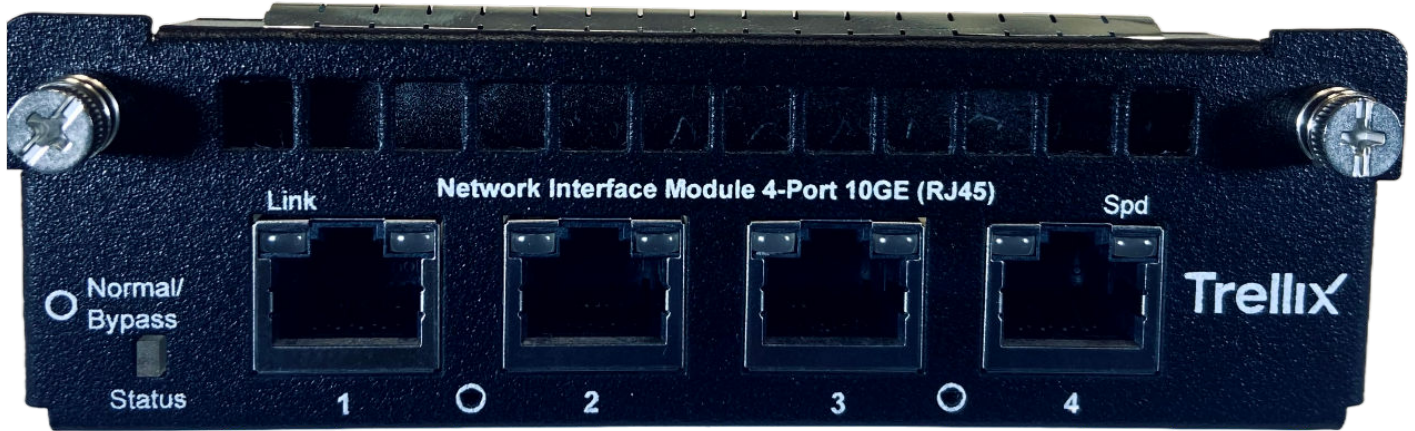
:

### 4-port RJ-45 10 Gbps/1 Gbps/100 Mbps with internal fail-open Network Interface Module

The 4-port RJ-45 with internal fail-open Network Interface Module provides 10 Gbps/1 Gbps/100 Mbps Ethernet performance on each port.

---

4-port RJ-45 10 Gbps/1 Gbps/100 Mbps with internal fail-open interface module



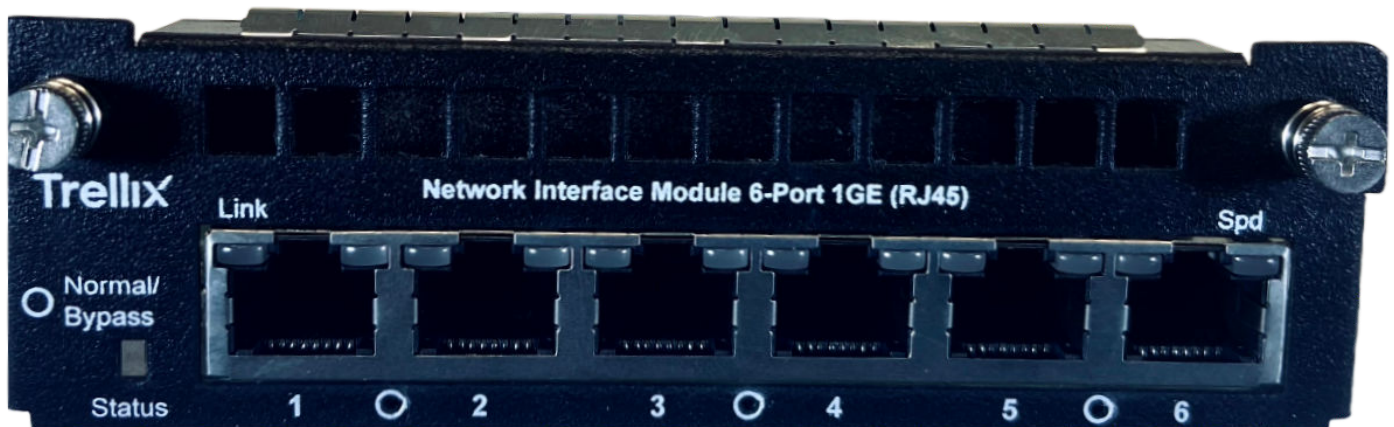
:

### 6-port RJ-45 1 Gbps/100 Mbps/10 Mbps with internal fail-open Network Interface Module

The 6-port RJ-45 with internal fail-open Network Interface Module provides 1 Gbps/100 Mbps/10 Mbps Ethernet performance on each port.

---

6-port RJ-45 1 Gbps/100 Mbps/10 Mbps with internal fail-open interface module



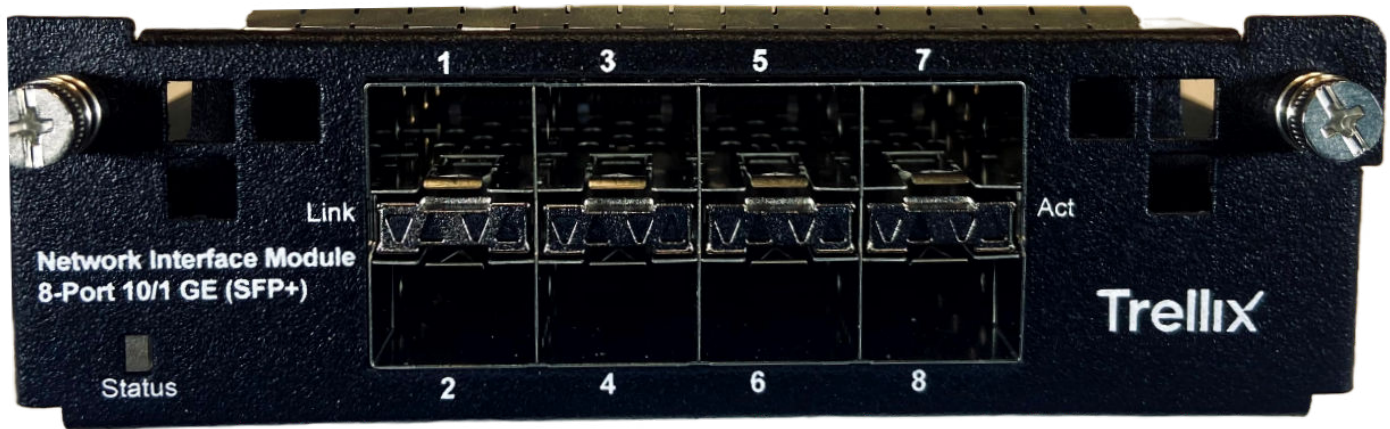
:

## 8-port SFP/SFP+ 1/10 Gigabit Network Interface Module

The 8-Port SFP/SFP+ (Small Form-Factor Pluggable Plus) Network Interface Module provides 1/10 Gigabit Ethernet performance on each port.

---

8-Port SFP+/SFP 10/1G Gigabit interface module



:

### Installation of the interface module

This section provides instructions on how to install the interface module based on the following scenarios:

- Install the interface module during a fresh installation of the Sensor.
- Install the interface module on an up and running Sensor.

:

### Install the interface module during a fresh installation of the Sensor

This section provides the steps to install the interface module for a fresh installation of Manager and Sensor.

1. Remove the module from its protective packaging.

#### Note

It is assumed that the Sensor is yet to be powered on, and trust between the Sensor and the Manager has not been established.

2. Grip the sides of the module with your thumb and forefinger and insert the module into the slot.

### Install an interface module



3. Drive in the screws fixed on the sides of the module to attach it to the Sensor.
4. Turn on the Sensor.
5. Establish trust between the Sensor and the Manager.

:

## Install the interface module on an up and running Sensor

This section provides the steps to install the interface module on a Sensor which is up and running.

1. Power on the Sensor without inserting the pluggable module(s) into the slot(s).
2. Establish trust between the Sensor and the IPS Manager.
3. Grip the sides of the module with your thumb and forefinger and insert the module into the slot.
4. Wait for 5 minutes.
5. Reboot the Sensor from the CLI.

:

## Remove an interface module

Perform these steps if you need to remove an interface module.

1. Disconnect the network fiber optic cable from the module.
2. Remove the transceivers from the module.
3. Unscrew the interface modules to detach them from the Sensor.
4. Place the module into its protective packaging.

:

## Small form-factor pluggable transceiver modules

The NS-series Sensors use two types of small form-factor pluggable transceiver modules as shown in the following table. For more information, see the section *NS-series Transceiver Modules* in *Trellix Intrusion Prevention System NS-series Reference Guide*.

Type	Performance
SFP	1 Gbps (copper) 1 Gbps (fiber optic)
SFP+	10 Gbps (fiber optic)

Each module is an input/output device that plugs into an LC-type Gigabit Ethernet port, linking the module port with a copper or fiber-optic network. SFP optical interfaces are less than half the size of GBIC interfaces.

To ensure compatibility, Trellix supports only those SFP, SFP+, QSFP+ and QSFP28 modules purchased through Trellix or from a Trellix-approved vendor. For a list of approved vendors, locate the relevant KnowledgeBase article at <https://supportm.trellix.com>. Enter the relevant KnowledgeBase article in Search the Support Knowledge Center and click Search to locate the article.

These installation instructions provide information for installing SFP and SFP+ modules that use a bail clasp for securing the module in place in the Sensor. Your module might be slightly different. Check the module manufacturer's installation instructions for more details. For ease of installation, insert the module in the Sensor while it is turned off and before placing it on a rack.

### Caution

To prevent eye damage, do not stare into open laser apertures.

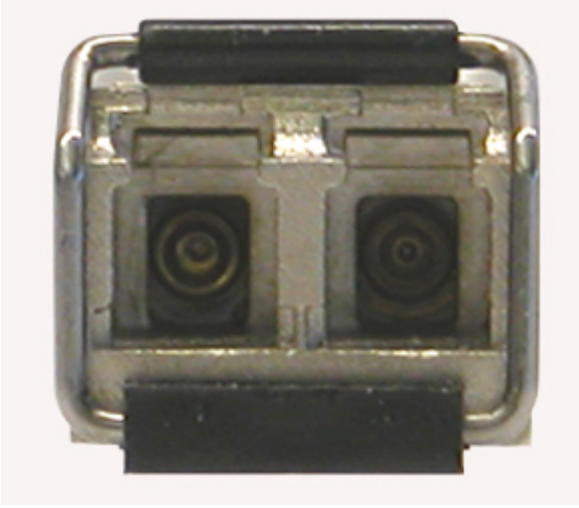
:

### SFP transceiver modules

An SFP module is a protocol-independent, compact, optical receiver, which allows for greater port density than the standard GBIC. This module operates at varying speeds for up to 1 gigabit per second on SONET/SDH, Fibre Channel, Gigabit Ethernet and other applications. An SFP module operates in multimode. Additionally, this module transmits on a 850-nanometer wavelength on short reach (SR) and 1310-nanometer long reach (LR).

---

An SFP module



:

### SFP+ transceiver modules

The enhanced small form-factor pluggable ( SFP+ ) is an enhanced version of the SFP that supports data rates up to 10 Gbps. 850nm SFP+ 1310nm SFP+Transceiver modules are supported.

850nm SFP+ transceiver module



1310nm SFP+ transceiver module



:

### Install a transceiver module

1. Remove the module from its protective packaging.



2. Locate the label on the module and make sure that the alignment groove is down.
3. Grip the sides of the module with your thumb and forefinger and insert the module into the module socket. Modules are keyed to prevent incorrect insertion.

---

Insert a transceiver module



:

### Remove a transceiver module

Perform these tasks if you need to remove a module.

#### Steps:

1. Disconnect the network fiber-optic cable from the module.
2. Release the module from the slot by pulling the bail clasp out of its locked position.
3. Slide the module out of the slot.
4. Insert the module plug into the module optical bore for protection.

:

## Attaching cables to the Sensor

Follow the steps outlined in this chapter to connect the cables to the various ports of your Sensor.

:

## Connect the cable to the Console port

The Console port on the NS-series Sensor is used for setup and configuration of the Sensor.

### Steps:

1. For console connections, plug the DB9 Console cable supplied by Trellix into the Console port on the Sensor. This port is labeled **Console** in the Sensor front panel.
2. Connect the other end of the Console port cable directly to a COM port of the computer or terminal server you will use to configure the Sensor, for example, a computer 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. Required settings for HyperTerminal are listed below:

Name	Setting
Baud rate	115200
Number of bits	8
Parity	None
Stop bits	1
Flow control	None

3. Turn on the Sensor.

:

## Connect the cable to the Response port

When operating in tap or SPAN mode, the Sensor uses its Response port to respond to attacks. When deployed in tap mode, the Sensor does not inject response packets through the tap but uses the Response port.

### Steps:

1. Plug a Cat-5e Ethernet cable into the Response port. This port is labeled **R1** on the Sensor rear panel.
2. Connect the other end of the cable to the network device, such as a hub, switch, or a router, through which you want to respond to attacks.

:

## Connect the cable to the Management port

The Sensor communicates with the Manager using the Management port.

1. Plug a Category 5e Ethernet cable into the Management port. This port is labeled **Mgmt** in the rear panel of the NS-series Sensor.
2. Plug the other end of the cable into the network device connected to your Manager server.

### Note

To isolate and protect your management traffic, Trellix strongly recommends you to use a separate, dedicated management subnet to interconnect the Sensors and the Manager.

:

## About connecting cables to the Monitoring ports

Connect to the network devices that you want to monitor through the Sensor monitoring ports. You can deploy Sensors in the following operating modes:

- In-line mode (fail-close)
- In-line mode (fail-open)
- Tap mode
- SPAN or hub mode

:

## How to use peer ports

You must use two peer Monitoring ports of the Sensor to deploy it full duplex mode. On the Sensor, the numbered ports are wired in pairs to accommodate the traffic.

The following Ethernet ports are coupled and must be used together.

### Note

- On NS7500 Sensors, G0 and G3 indicate the fixed port slots. G1 and G2 indicate the slots for interface modules.
- In the following table, it is assumed that G1 is a 6-port RJ-45 1000/100/10 Mbps interface module and G2 is the 8-Port SFP+/SFP 10/1 Gigabit interface module. These interface modules can be interchanged.
- Since monitoring ports are internally wired, when you disable one of the ports in a pair, the corresponding port is also disabled.

Port Pairs	Sensor
G0/1 and G0/2	NS7500
G1/1 and G1/2	NS7500
G1/3 and G1/4	NS7500
G1/5 and G1/6	NS7500
G2/1 and G2/2	NS7500
G2/3 and G2/4	NS7500
G2/5 and G2/6	NS7500
G2/7 and G2/8	NS7500
G3/1 and G3/2	NS7500
G3/3 and G3/4	NS7500
G3/5 and G3/6	NS7500
G3/7 and G3/8	NS7500

:

## Cable types for routers, switches, hubs, and computers

This section lists the types of cables that you require to connect the Sensor to other network devices:

- Use a straight/crossover Ethernet RJ-45 cable to connect a router port to computer to the Sensor Management port.
- Use a straight/crossover Ethernet RJ-45 cable to connect a computer to the Sensor monitoring port.

:

## Connect the cables for in-line mode

In-line Gigabit Ethernet ports can be configured as fail-open or fail-closed. The RJ-45 monitoring ports are built-in and include an built-in fail-open functionality as well. All other monitoring ports require the use of either Trellix's 4-port 1/10 Gigabit Modular Passive Fail-Open kit or external active fail-open (AFO) kits for In-Line Fail-Open Active configuration.

The 8-port SFP+ module and its monitoring ports require the use of external active fail-open for fail-open functionality.

Gigabit Ethernet ports fail-close, means the flow of traffic will stop if the Sensor fails. To allow traffic to flow uninterrupted, you must use special hardware, and cable the Sensor to external active fail-open kits. For instructions, see the subsequent sections of this chapter.

This section provides the steps to connect the Sensor's Gigabit Ethernet ports so they fail-close.

1. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports, for example G3/1.
2. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports, for example G3/2.



3. 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).

:

## Connect the cables for tap mode

To deploy the Sensor in tap mode, you must use a Sensor's Gigabit Ethernet Monitoring port pair with a third-party external tap.

### Note

For a list of Trellix-approved third party vendors, see the KnowledgeBase at <https://supportm.trellix.com>. Enter the relevant KnowledgeBase article in Search the Support Knowledge Center and click Search to locate the relevant KnowledgeBase article.

### Steps:

1. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports, for example, G1/1.

2. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports labeled G1/2.
3. Connect the other end of each cable to the tap.
4. Connect the network devices that you want to monitor to the tap.

:

### Connect the cables for SPAN or hub mode

For the Sensor, monitoring in SPAN or hub mode occurs in in-line fail-open mode. When you monitor in SPAN or hub mode, you use only single ports.

To connect an Sensor to a SPAN port or hub, plug an LC fiber-optic or RJ-45 cable into one of the modules and connect the other end of the cable to the SPAN port or the hub.

:

### Connect the cable for Sensor failover

For Sensor failover, connect two NS7500 Sensors using the standard LC-LC cables. These two Sensors must be running the same software version.

Purchase two 10G SFP+ and use the standard cables. Failover cables are additional hardware required to support failover communication between two NS7500 Sensors.

#### Note

Trellix does not ship the transceiver modules and cables with the NS7500 Sensors. Please purchase the same separately for failover setup.

Refer to the following table before you configure a HA pair:

Sensor Model	Port to connect the HA pair	Cable requirements for failover
NS7500	G0/1	2 10G SFP+ and standard LC-LC cable

#### Steps:

1. Plug the cable appropriate for use with your SFP+ module into port G0/1 of the active NS7500 Sensor.
2. Connect the other end of the cable with SFP+ into port G0/1 of the standby NS7500 Sensor.

:

## Connect the cables for Sensor Fail-Open

The Fail-Open Kits minimize the potential risks of in-line Sensor failure on critical network links. You need to purchase these kits separately. Both copper and optical versions of the kit are available for the one-gigabit ports. The standard Gigabit Fail-Open Kits and 10 Gigabit Fail-Open Kits are available for the 1 and 10 gigabit ports respectively.

The Monitoring ports of the Sensors can be fail-close; thus, if the Sensor is deployed in-line fail-close, a hardware failure results in network downtime. Except the built-in RJ-45 ports which come with built-in fail-open functionality, you use either the optional Trellix's 4-port 1/10 Gigabit Modular Passive Fail-Open kit or external bypass switch provided in an Active Fail-Open Kit for the Monitoring ports to fail-open.

While the Sensor is operating, the Active Fail-Open kit is in-line and routes all traffic directly through the Sensor. When the Sensor fails, the switch automatically shifts to a bypass state; in-line traffic continues to flow through the network link but is no longer routed through the Sensor. After the Sensor resumes normal operation, the switch returns to the "on" state, once again enabling in-line monitoring. The port pairs with Active Fail-Open kits resume inline mode after a Sensor resumes normal operation or is in good health.

- G0 supports passive fail-open mode with RJ-11 port control

### Note

G0 also supports active fail-open using a Copper and Fiber 1/10 Gigabit Active Fail-Open kit.

- G1 and G2 supports built-in fail-open and active fail-open mode for these interface modules:
  - 4-port 10 GigE/1 GigE LR Optical with internal fail-open
  - 4-port 10 GigE/1 GigE SR Optical 50 micron with internal fail-open
  - 4-port 10 GigE/1 GigE SR Optical 62.5 micron with internal fail-open
  - 4-port RJ-45 10 GigE with internal fail-open
  - 6-port RJ-45 1 GigE with internal fail-open

### Note

All RJ-45 ports support active fail-open using only a Copper Active Fail-Open kit.

- 8-port SFP/SFP+ 1/10 Gigabit

### Note

The 8-port module supports active fail-open using a Copper and Fiber 1/10 Gigabit Active Fail-Open kit.

- G3 supports both internal fail-open and active fail-open mode when connected to an Active Fail-Open (AFO) kit

 **Caution**

Sensor outage breaks the link connecting the devices on either side of the Sensor for a brief moment and requires the renegotiation of the network link between the two peer devices connected to the Sensor. Depending on the network equipment, this disruption introduced by the renegotiation of the link layer between the two peer devices might range from a couple of seconds to more than a minute with certain vendors' devices.

 **Caution**

A very brief link disruption might also occur while the links between the Sensor and each of the peer devices are renegotiated to place the Sensor back in in-line mode. This outage, again, varies depending on the device, and can range from a few seconds to more than a minute.

The performance of the switchover from in-line to bypass and vice versa varies depending on the vendor.

You can find the installation and troubleshooting instructions for the kit in the guide that accompanies the kit. For example, for information on the Modular kits, see the following guides:

- *1/10 Gigabit Modular Active Fail-Open Bypass Kit Guide*
- *1/10 Gigabit Modular Passive Fail-Open Bypass Kit Guide*

:

## Turning the Sensor on and off

 **Note**

Do not attempt to turn on the Sensor until you have installed the Sensor in a rack and made all the necessary network connections.

### Steps:

1. Connect the power cable to the Sensor power supply.
2. Connect the power cable to a power source.

 **Note**

If you are installing a redundant power supply, you should install it as described in *Install a new power supply* section. For true redundant operation with the optional redundant power supply, Trellix recommends that you plug each supply into a different power circuit.

The Sensor has no power switch. The Sensor turns on as soon as one of its power cables is connected to a power source. Trellix recommends that you use the **shutdown** CLI command to halt the Sensor before turning it off. For more



information on *CLI commands*, see the *CLI commands* section in *Trellix Intrusion Prevention System Product Guide* for specific Sensor software version you are running.

:

### 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**. Additional or upgraded license is required to increase the throughput of the Sensor.

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 capacity licenses available for the NS7500 Sensors:

License SKUs	Throughput	No of Sensors
NS75X03CAE-AT	3 Gbps	1 NS7500 Sensor
NS75X05CAE-AT	5 Gbps	1 NS7500 Sensor
NS75X075CAE-AT	7.5 Gbps	1 NS7500 Sensor

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

License SKUs	Throughput	No of Sensors
NS75X35CAE-DT	3 to 5 Gbps	1 NS7500 Sensor
NS75X375CAE-DT	3 to 7.5 Gbps	1 NS7500 Sensor
NS75X575CAE-DT	5 to 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 licenses, see [Managing licenses for NS7500 Sensors](#).

:

## License requirement for NS7500 Sensor failover

Based on the throughput, the NS7500 Sensor requires an additional license for Sensor failover. To obtain a license, contact **Trellix Sales**.

The table below shows the capacity licenses available for the NS7500 Sensor failover:

License SKUs	Throughput	Number of Sensors
FO75X03CAE-AT	3 Gbps	2 * 1 NS7500 Sensor
FO75X05CAE-AT	5 Gbps	2 * 1 NS7500 Sensor
FO75X075CAE-AT	7.5 Gbps	2 * 1 NS7500 Sensor

The table below shows the upgrade capacity licenses available for the NS7500 Sensor failover:

License SKUs	Throughput	Number of Sensors
NS75XF35CAE-DT	3 to 5 Gbps	2 * 1 NS7500 Sensor
NS75XF375CAE-DT	3 to 7.5 Gbps	2 * 1 NS7500 Sensor
NS75XF575CAE-DT	5 to 7.5 Gbps	2 * 1 NS7500 Sensor

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

:

## Managing licenses for NS7500 Sensors

The NS7500 Sensor requires a license to activate the baseline throughput of 3 Gbps. Additional license is required to increase the throughput from 3 Gbps to 5 Gbps or 7.5 Gbps. The license is provided as a .zip or .jar file.

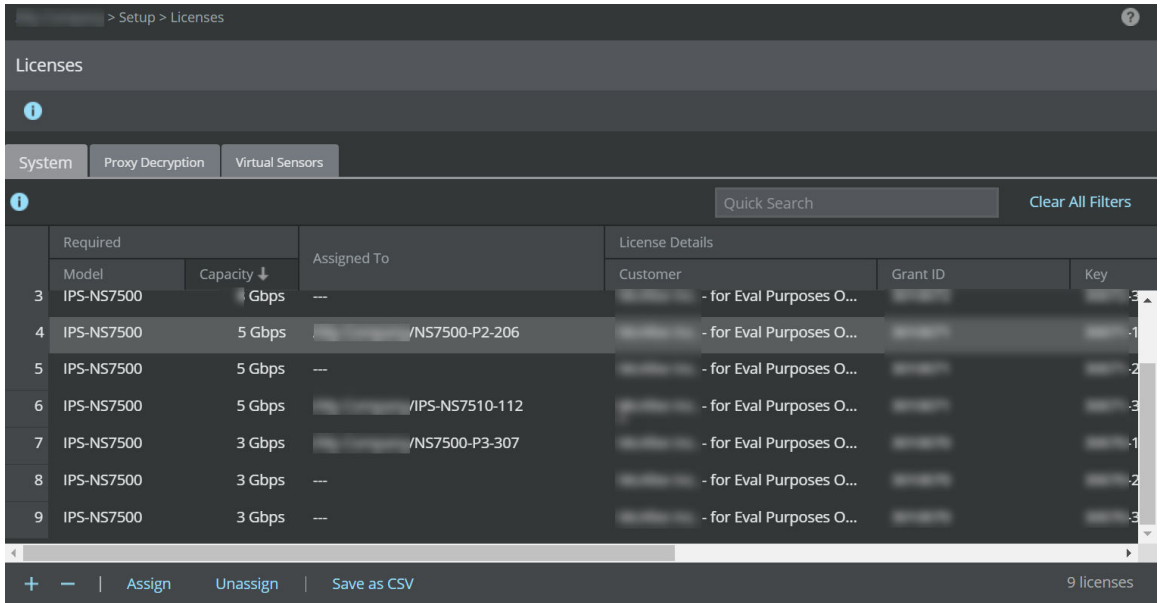
### Note

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






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

The following details are displayed on the System tab:

Upload license capacity for Sensor



Option	Definition
Required	Model – Sensor model compatible with the license Capacity – Throughput limit for the license
Assigned To	Name of the Sensor assigned to the license
License Details	Customer – Customer for whom the license file was generated Grant ID – Trellix Grant ID of the corresponding customer Key – License key number of the customer. Expiration – Applicable only for demo and subscription licenses

Option	Definition
	<ul style="list-style-type: none"> <li>• : Valid license</li> <li>• : Expired license</li> <li>• : Expired license running on grace period</li> </ul> <p> <b>Note:</b> A grace period of <b>30 days</b> is provided to subscription-based System licenses after they expire.</p> <p>Post grace period, the Sensor continues to inspect traffic, and operates with the existing signature set and configuration. The Manager, however, will not be able to deploy new signature sets or policies to the Sensor until a valid license is assigned.</p> <p>Type - Displays if the license is Perpetual, Subscription, or Evaluation (Demo) type.</p> <p> <b>Note:</b> It is recommended to install subscription license from Manager version 10.1.7.44 and later.</p>
Added	<p>Time - Date in &lt;mm-yy&gt; format, and time when the license was added</p> <p>By - Name of the user who added the license</p>
Comments	<p>Enables you to add your comment per license file that is imported. Double-click in the Comment field and enter your comment. Click outside this field and your comment is automatically saved.</p>

The following actions can be performed on the System tab:


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

- [Remove a license from the Manager](#)

:

## Add license to the Manager

To upload the license, perform the following steps:

1. Go to Manager → <Admin Domain Name> → Setup → Licenses.
2. Click the System tab.
3. Click .

The Add License pop-up window opens.

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

### Note

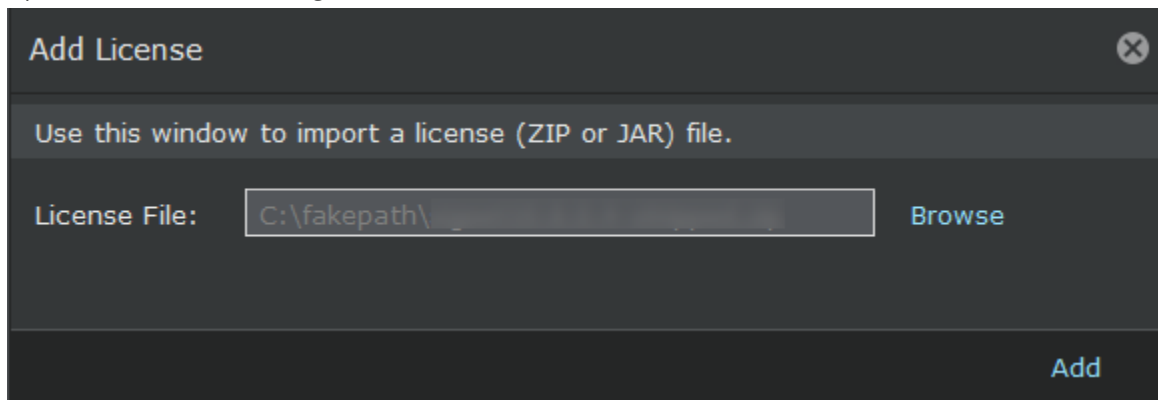
The supported license formats are .zip and .jar.

### Note

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

---

Upload license to the Manager



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

:

## Assign a license to a Sensor

To assign the license to the Sensor, perform the following steps:

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

Required		Assigned To	License Details				
Model ↑	Capacity		Customer	Grant ID	Key	Expiration	Type
1	IPS-NS7500	5 Gbps	---	---	---	✓ Sep 12 2025	Subscription
2	IPS-NS7500	7.5 Gbps	---	---	---	---	Perpetual
3	IPS-NS7500	7.5 Gbps	---	---	---	---	Perpetual
4	IPS-NS7500	7.5 Gbps	---	---	---	---	Perpetual
5	IPS-NS7500	7.5 Gbps	---	---	---	---	Perpetual
6	IPS-NS7500	7.5 Gbps	---	---	---	---	Perpetual
7	IPS-NS7500	7.5 Gbps	---	---	---	---	Perpetual

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

**Assign License**

Model: IPS-NS7500

Capacity: 3 Gbps

Grant ID: [redacted]

Key: [redacted]

Expiration: ✓ Dec 31 [redacted]

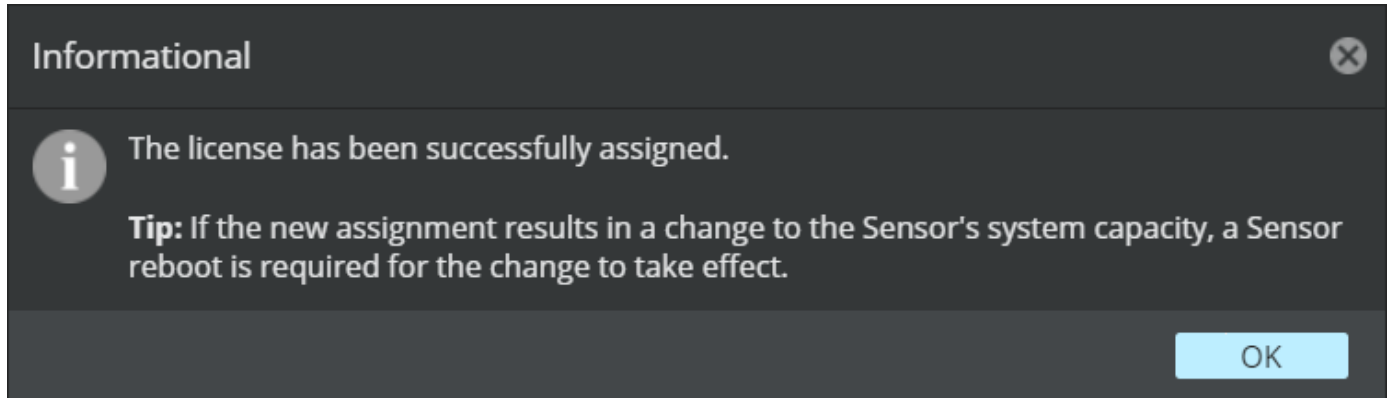
Assign To: /My Company/NS7500\_107

Assign

 Note

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

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

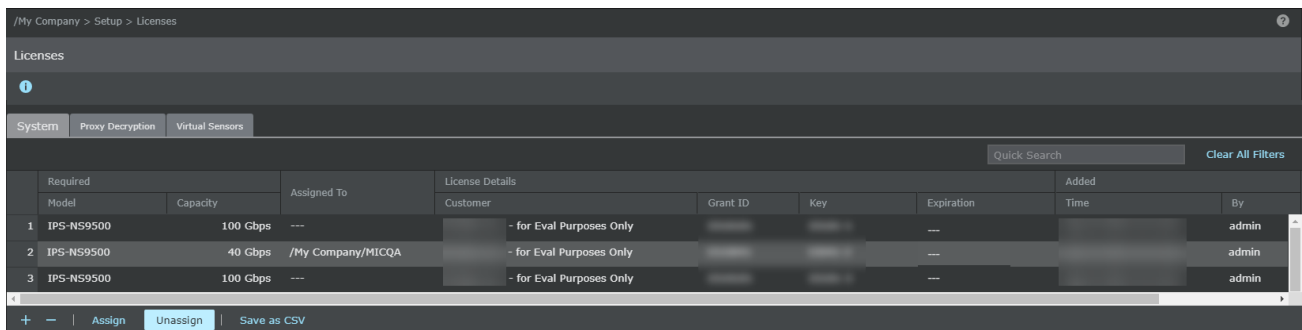
 Note

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

## Unassign a license from a Sensor

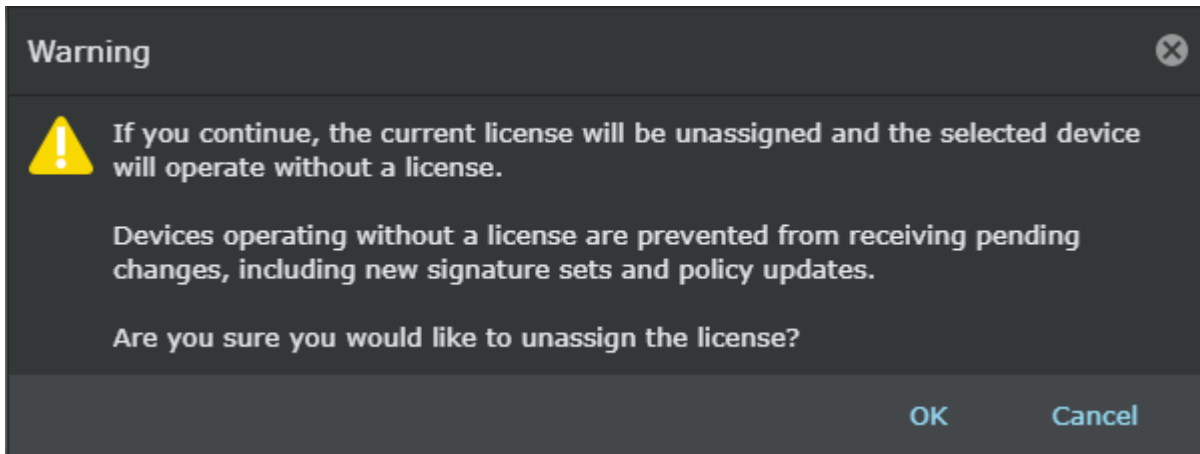
To unassign the license, perform the following steps:

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



4. Click Unassign.

5. Click Ok.



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

:

## Upgrade an existing capacity license

### Note

This section is not applicable to Sensors running on subscription based licenses. It is applicable only for Sensors running with perpetual licenses.

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

#### Steps:

1. Go to Manager → <Admin Domain Name> → Setup → Licenses.
2. Click the System tab. The system tab with existing licenses:



Required		Assigned To	License Details		
Model	Capacity ↓		Customer	Grant ID	Key
1	IPS-NS7500	5 Gbps	---	- for Eval Purposes O...	
2	IPS-NS7500	5 Gbps	---	- for Eval Purposes O...	
3	IPS-NS7500	5 Gbps	/NS7...	- for Eval Purposes O...	
4	IPS-NS7500	3 Gbps	---	- for Eval Purposes O...	
5	IPS-NS7500	3 Gbps	---	- for Eval Purposes O...	
6	IPS-NS7500	3 Gbps	---	- for Eval Purposes O...	

3. Click .

The Add License pop-up window opens.

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

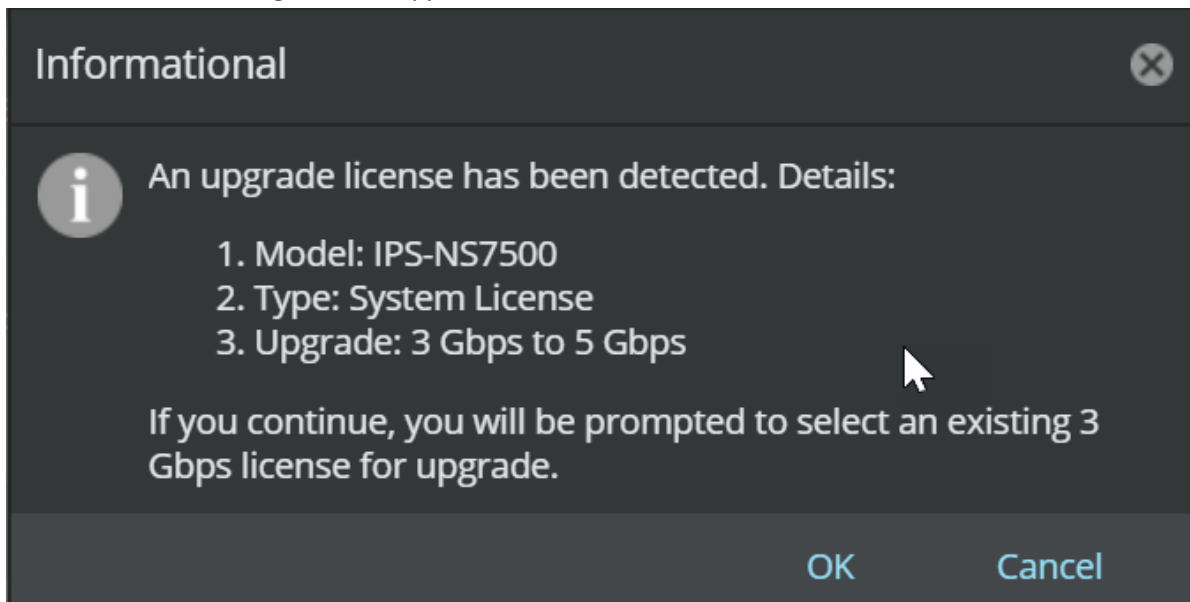
#### Note

The supported license formats are .zip and .jar.

#### Upload license to the Manager

5. Click Add.

- a. An informational message window appears. Click OK.

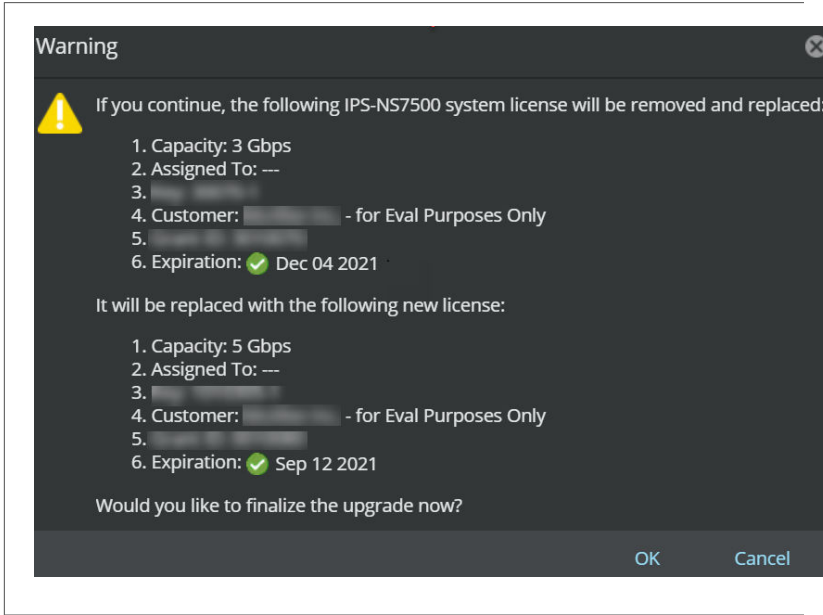


- b. <Sensor name> System license upgrade (from x Gbps to x+y Gbps) window appears which displays all the licenses present in the Manager for that particular capacity. Double-click on the license you wish to upgrade the capacity license for.

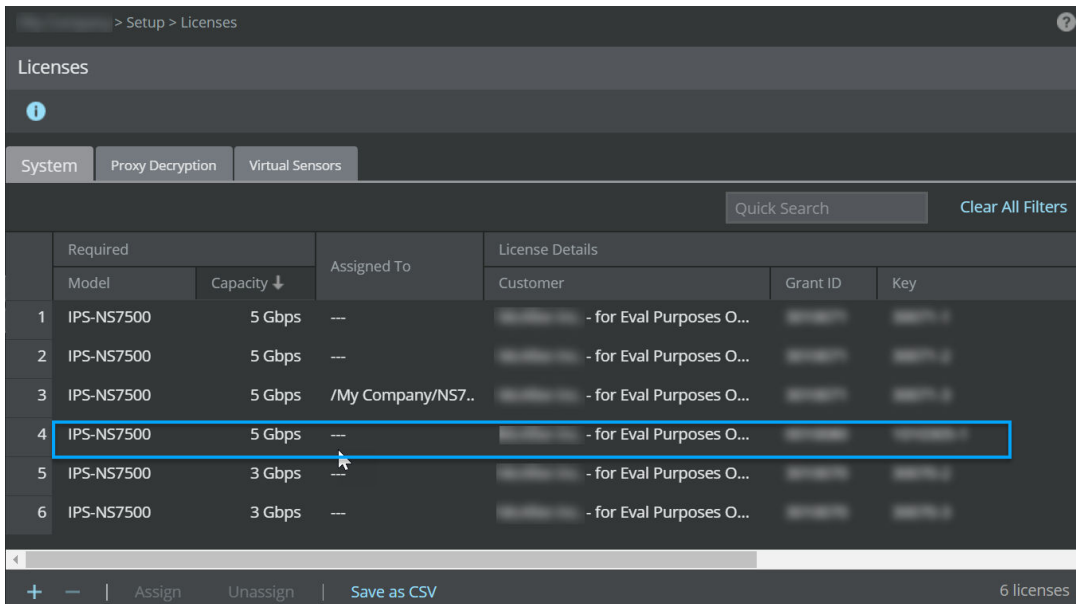
The image shows a window titled "IPS-NS7500 System License Upgrade (from 3 Gbps to 5 Gbps)" with a close button (X) in the top right corner. Below the title bar is an information icon (i) and a "Quick Search" input field. The main content is a table with the following structure:

	Required		Assigned To	License Details		
	Model	Capacity ↓		Customer	Grant ID	Key
1	IPS-NS7500	3 Gbps	---	- for Eval Purposes O...		
2	IPS-NS7500	3 Gbps	---	- for Eval Purposes O...		
3	IPS-NS7500	3 Gbps	---	- for Eval Purposes O...		

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



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




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

:

### Remove a license from the Manager

To remove a license, perform the following steps:

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

:

## Troubleshooting the Sensor

This section lists some common installation problems, the possible causes, and the corresponding solutions.

Problem	Possible Cause	Solution
LED is off.	The Sensor is turned off.	Restore Sensor power.
LED is off.	The Sensor port cable is disconnected.	Check the Sensor cable connections.
Sensor is operational but is not monitoring traffic.	Network device cables have been disconnected.	Check the cables and make sure they are properly connected to both the network devices and the bypass switch.
Sensor is operational but is not monitoring traffic.	The Sensor ports have not been enabled in the Manager.	The Sensor will not monitor traffic on the ports unless the ports are enabled in the Manager. Ports are disabled in case of Sensor failure; you must re-enable them for Sensor monitoring to resume.

Problem	Possible Cause	Solution
Network or link problems	Improper cabling or port configuration	Make sure that the transmitting and receiving cables are properly connected to the bypass switch.
Runts or giants errors on switch and routers	Improper cabling or port configuration	Make sure that the transmitting and receiving cables are properly connected to the bypass switch.
The system fault "Switch absent" appears on Faults tab in the Logs page.	The Active Fail-Open Kit is disconnected.	Check the Active Fail-Open Kit and make sure it is properly connected to the Sensor.

:

## Sensor technical specifications

The following table lists the specifications of for N7500 Sensors.

Sensor Specifics	NS7500
Dimensions	17.31" (W) x 1.75" (H) x 29.13" (D)
Weight	25.5 lbs
Storage	240 GB M.2 drive
<b>System Heat Dissipation</b>	
Maximum BTU	1023 BTU/hr
Typical BTU	852 BTU/hr
Maximum Power Consumption	300W

Sensor Specifics	NS7500
Typical Power Consumption	250W
Redundant Power Supply	Yes
Power	100 - 240 VAC (50 - 60 Hz)
DC Power Supply	<p>Installing DC power supply is optional.            Maximum Power Consumption: 598 W            Maximum BTU: 2038 BTU/hr            Power Supply Unit:</p> <ul style="list-style-type: none"> <li>• Input V: - 40 to -72 V</li> <li>• Input A: 12.45 A</li> </ul>
Temperature	Operating: 0° to 35° C , Non-operating: - 40° to 70° C
Relative humidity (non-condensing)	Operational: 10% to 90%, Non-operational: 5% to 95%
Altitude	0 to 10,000 feet
Safety Certification	UL 60950-1 (USA); CSA 22.1.No. 60950-1 (Canada); EN 60950-1 (Europe); CNS 14336-1 (Taiwan), GB 4943-1 (China); IEC 60950-1 (International) - CB Scheme certificate and test report covering all applicable country deviations; IEC 60825 and 21CFR1040
EMI Certification	FCC Part 15 Subpart B Class A (USA); CAN ICES-3 Class A (Canada); EN 55022, EN 55032, EN 55024, EN61000-3-2, EN61000-3-3 (Europe and International); VCCI Class A (Japan); AS/NZS CISPR 32 (Australia and New Zealand); CNS 13438 (Taiwan); GB 9254-2008 (China); KN32 and KN35 (South Korea); GB 17625.1 (China)

:

## NS7x50 Sensors

:

### About Sensors

Sensors are high-performance, scalable, and flexible content processing appliances built for the accurate detection and prevention of:

- Network intrusions
- Network misuse
- Distributed Denial-of-Service (DDoS) attacks

Sensors are specifically designed to handle traffic at wire speed, efficiently inspect and detect intrusions with a high degree of accuracy, and flexible enough to adapt to the security needs of any enterprise environment. When deployed at key network access points, the Sensor provides real-time traffic monitoring to detect malicious activity and respond to the malicious activity as configured by the administrator.

After you deploy a Sensor successfully, you configure and manage it using the Manager. The process of configuring a Sensor and establishing communication with the Manager is described in the subsequent chapters of this guide. For the details about the Manager, see the *Manager Administration* section in *Trellix Intrusion Prevention System Product Guide*.

:

### Functions of an NS-series Sensor

The NS-series Sensors are a third-generation hardware platform for Sensors designed for high bandwidth links to offer Next Generation IPS (NGIPS) capability and provide high aggregate throughput across various Sensor models. The following models are supported.

- NS7350 - The NS7350 Sensor is a 1RU unit, providing an aggregate throughput of 5 Gbps
- NS7250 - The NS7250 Sensor is a 1RU unit providing an aggregate throughput of 3 Gbps
- NS7150 - The NS7150 Sensor is a 1RU unit providing an aggregate throughput of 1.5 Gbps

The primary function of a Sensor is to analyze traffic on selected network segments and to respond when an attack is detected. The Sensor examines the header and data portion of every network packet, looking for patterns and behavior in the network traffic that indicate malicious activity. The Sensor examines packets according to user-configured policies, or rule sets, which determine what attacks to watch for, and how to respond with countermeasures if an attack is detected.

If an attack is detected, a Sensor responds according to its configured policy. Sensor can perform many types of attack responses, including generating alerts and packet logs, resetting TCP connections, "scrubbing" malicious packets, and even blocking attack packets entirely before they reach the intended target.

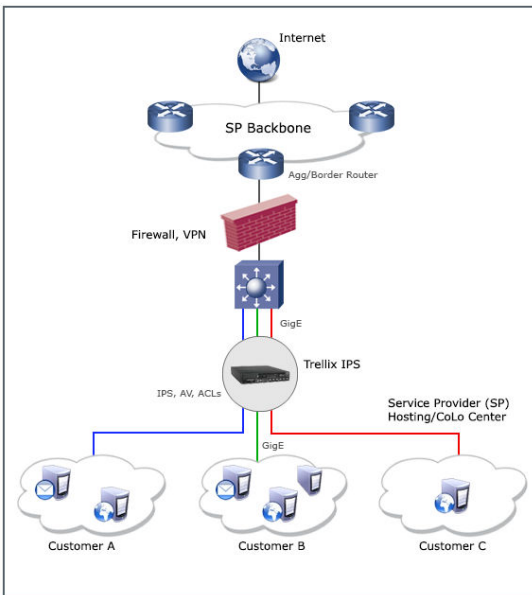
:

## Deployment of an NS-series Sensor

Deployment of a Sensor requires knowledge of your network to help determine the level of configuration and the number of installed Sensors. You also need to determine the number of Trellix ePolicy Orchestrator - On-prem servers required to protect your network. The Sensor is purpose-built for the monitoring of traffic across one or more network segments.

Following is an example of a network topology using Gigabit Ethernet throughput. In the illustration, Trellix Intrusion Prevention System provides IPS protection to outsourced servers. High port-density and virtualization provides a highly scalable solution, while Trellix IPS protects against web and eCommerce mail server exploits.

### A sample NS-Series deployment



:

## NS7x50 Sensor physical description

The high-port density NS-series Sensor is designed for high bandwidth links. This section gives a physical description of the NS7x50 Sensors.

The NS7350, NS7250, and NS7150 Sensor models are a mid-range offering that provide 5 Gbps, 3 Gbps, and 1.5 Gbps throughput respectively.

:

## Components of an NS7x50 Sensor

The NS7x50 front and rear panel details are described below.



## The NS7150/NS7250/NS7350 Sensor model

### Sensor front panel



1. Console port (1)
2. RJ-11 port (1) for passive fail-open control of two built-in SFP+ ports in slot G0. The RJ-11 port supports 1 Gbps (SFP) copper or fiber and 10 Gbps (SFP+) (SR and LR).
3. SFP+ 1/10 Gigabit Ethernet ports (2)

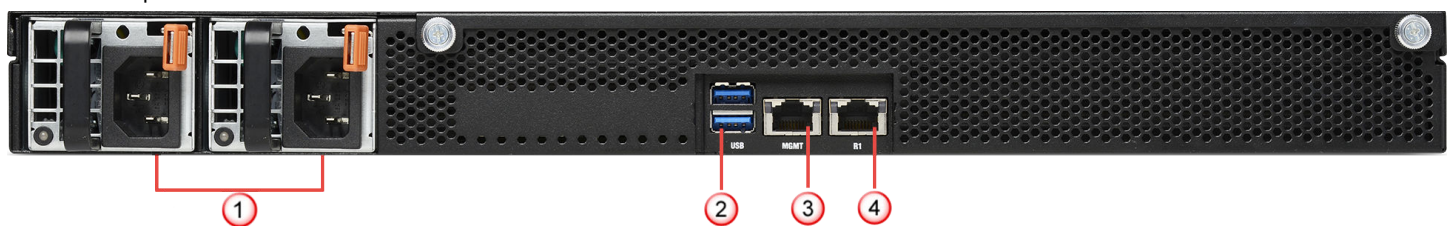
### **i** Important

The RJ-11 port controls only the G0 SFP+ 1/10 port pair in passive fail-open mode.

4. Two slots for I/O modules (Any combination of the interface modules can be used)
  - RJ-45 10/100/1000 Mbps with internal fail-open Ethernet Monitoring ports (6)
  - RJ-45 10 Gbps/1 Gbps/100 Mbps with internal fail-open Network Interface Module (4)
  - SFP/SFP+ 1/10 GigE Monitoring ports (8)
  - SFP/SFP+ 10/1 GigE SM 8.5 micron with internal fail-open Monitoring ports (4)
  - SFP/SFP+ 10/1 GigE MM 50 micron with internal fail-open Monitoring ports (4)
  - SFP/SFP+ 10/1 GigE MM 62.5 micron with internal fail-open Monitoring ports (4)
5. RJ-45 10/100/1000 Mbps Ethernet Monitoring ports (8)

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

### Sensor rear panel



1. Power supply inlet (2)
2. USB ports (2)
3. RJ-45 10 Gbps/1 Gbps Management port (Mgmt) (1)
4. RJ-45 10 Gbps/1 Gbps Response port (R1) (1)

The NS7x50 Sensors have five fan units on the top.

Fan units-NS7150/NS7250/NS7350



The direction of airflow in all the Sensors is front to back. Cold air enters through the front of the chassis.

 **Note**

The fan units and power supplies are field replaceable.

The following table gives the details of the supported ports.

Ports	NS7150/NS7250/NS7350
Fixed Gigabit Ethernet—Copper ports (internal fail-open)	8
Fixed 10 GigE/1 GigE (SFP+) ports	2
Network I/O slots	2
Network I/O modules	4-port 10/1 GigE SM 8.5 micron with internal fail-open 4-port 10/1 GigE MM 50 micron with internal fail-open 4-port 10/1 GigE MM 62.5 micron with internal fail-open

Ports	NS7150/NS7250/NS7350
	4-port RJ-45 10 GigE with internal fail-open 6-port RJ-45 1 GigE with internal fail-open 8-port (SFP+/SFP) 10/1 GigE
10 Gigabit Ethernet	Modular up to 18
Dedicated Response ports (RJ-45)	1 (10G/1G)
Dedicated Management ports (RJ-45)	1 (10G/1G)
USB ports	2

- **Console port** — Use to set up and configure the Sensor using the CLI.
- **RJ-11 port** — Controls the SFP+ 1/10 Gigabit Ethernet port pair in passive fail-open mode
- **SFP/SFP+ 1/10 Gigabit Ethernet ports** — Enables to monitor two SPAN ports, two segments in-line, or a combination
- **RJ-45 10/100/1000 Mbps Ethernet Monitoring ports** — Enables to monitor eight SPAN ports, four segments in-line, or a combination
- **External USB ports** — Use these in troubleshooting situations for system recovery purposes. You need to restart the Sensor through the USB storage device.
- **RJ-45 10G/1G Management port**— Use for communication with the Manager server. You can assign an IP address to this port during installation.
- **RJ-45 10G/1G Response port** — When you're operating in SPAN or tap mode, it enables you to inject response packets back through a switch or router.
- **Power Supply** — Power supply is included with an NS7x50 Sensor. The supply uses a standard IEC port (IEC320-C13). Trellix provides a standard, 2m NEMA 5-15P (US) power cable (3 wire). International customers must procure a country-appropriate power cable.

The NS-series Sensor does not have internal taps; you must use it with a third-party external tap to run it in tapped mode.

:

## Sensor LEDs

The front and rear panel LEDs provide status information for the health of the Sensor and the activity on its ports. The following table describes the NS-series LEDs.

## Front panel LEDs

LED	Status	Description
Status	Green Amber	Sensor is operating in good health. Sensor is booting up. It also indicate a system bad health.
Fan	Green Amber	All the fans are operating. One or more fans are not working.
Temp	Green Amber	Inlet air temperature measured inside the chassis is normal. (Chassis temperature OK) Inlet air temperature measured inside the chassis is too high. (Chassis temperature too hot)
Gigabit Ports Act	Blinking Amber Off	Data is received or transmitted. No data is being transferred.
Gigabit Ports Link	Green Off	The link is up. The link is down.
Normal/Bypass	Green Off	The port pair is in Inline Fail-Open/Inline Fail-Close/SPAN/Tap Mode. The Port Pair is in the Bypass Mode.

## Rear panel LEDs

LED	Status	Description
Power	Solid Green Blinking Green Solid Amber	Power Supply is functioning Power Supply is stand-by. It also indicates load sharing. Power Supply is not functioning or the unit has no power feed.
Management Port Speed	Green Amber	The port speed is 10 Gbps. The port speed is 1 Gbps.
Management Port Link	Green Off	The link is up. The link is down.
Response Port Speed	Green Amber	The port speed is 10 Gbps. The port speed is 1 Gbps.
Response Port Link	Green Off	The link is up. The link is down.

:

## Before you install

This chapter describes the best practices for deployment of Sensors in your network. Topics include the safety considerations for handling the Sensor, usage restrictions that apply to the Sensor model, and the contents that are shipped along with the Sensor.

:

### Usage restrictions

The following restrictions apply to the use and operation of a Sensor:

- You should not remove the outer shell of the Sensor. If you do so, this will invalidate your warranty.
- The Sensor appliance is not a general purpose workstation.
- Trellix prohibits the use of the Sensor appliance for anything other than operating Network Security Platform.

- Trellix prohibits the modification or installation of any hardware or software on the Sensor appliance that is not part of the normal operation of Network Security Platform.

:

### Safety measures

Please read the following warnings before you install the Sensor. These safety measures apply to all Sensor models unless otherwise noted. Failure to observe these safety warnings could result in serious physical injury.

### Warnings:

- Read the installation instructions before you connect the system to its power source.
- To remove all power from the Sensor, unplug all power cords, including the redundant power cord.
- Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
- Before working on the equipment that is connected to power lines, remove all jewelry including rings, necklaces, and watches. Metal objects will heat up when connected to power and ground, and can cause serious burns or weld the metal object to the terminals.
- This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.
- Do not remove the outer shell of the Sensor. Doing so will invalidate your warranty.
- Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Blank faceplates and cover panels prevent exposure to hazardous voltages and currents inside the chassis, contain electromagnetic interference (EMI) that might disrupt other equipment and direct the flow of cooling air through the chassis.
- To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the users will be required to correct the interference at their own expense.
- Refer to the Appendix for information on regulatory, compliance, and other safety requirements.

:

### About fiber-optic ports

The Sensor uses fiber-optic connectors for its Monitoring ports. The connector type is an SFP/SFP+ fiber optic connector that is LC-duplex compatible.

Note the following:

- Fiber-optic ports (for example, SFP/SFP+, FDDI, OC-3, OC-12, OC-48, ATM, GBIC, and 100BaseFX) are considered Class 1 laser or Class 1 LED ports.
- These products have been tested and found to comply with Class 1 limits of IEC 60825-1, IEC 60825-2, EN 60825-1, EN 60825-2, and 21CFR1040.

### Caution

To avoid exposure to radiation, do not stare into the aperture of a fiber-optic port. Invisible radiation could be emitted from the aperture of the port when no fiber cable is connected.

- Only FDA registered, EN 60825-1 and IEC 60825-1 certified Class 1 SFP/SFP+/ laser transceivers are acceptable for use with the Sensor.

:

## Contents of 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

:

## Unpack the Sensor

Steps:

1. Open the crate.
2. Remove the first accessory box.
3. Verify you have received all parts. These parts are listed on the packing list and in the *Contents of the box* section.
4. Remove the Sensor.
5. Place the Sensor box as close to the installation site as possible.
6. Position the box with the text upright.
7. Open the top flaps of the box.
8. Remove the accessory box within the Sensor box.
9. Verify you have received all parts. These parts are listed on the packing list and in the *Contents of the box* section.
10. Remove the Slide Rail Kit.
11. Pull out the packing material surrounding the Sensor.
12. Remove the Sensor from the antistatic bag.
13. Save the box and packing materials for later use in case you need to move or ship the Sensor.

:

## Setting up the Sensor

This chapter describes how to set up the Sensor for you to configure it.

:

### Setup overview

Setting up a Sensor involves these steps:

1. Position the Sensor.
2. Install interface modules (SFP and SFP+).
3. Attach power, network, and monitoring cables.
4. Turn on the Sensor.
5. Configure the Sensor after you have set up and turned it on.

:

### How to position the Sensor

Place the Sensor in a physically secure location, close to the switches or routers it will be monitoring. Ideally, the Sensor should be located within a standard communications rack. To mount the Sensor on a rack, you will attach two mounting rails to the Sensor as described in the subsequent sections of this guide.

:

### Install the slide rails and rack-mount the Sensor

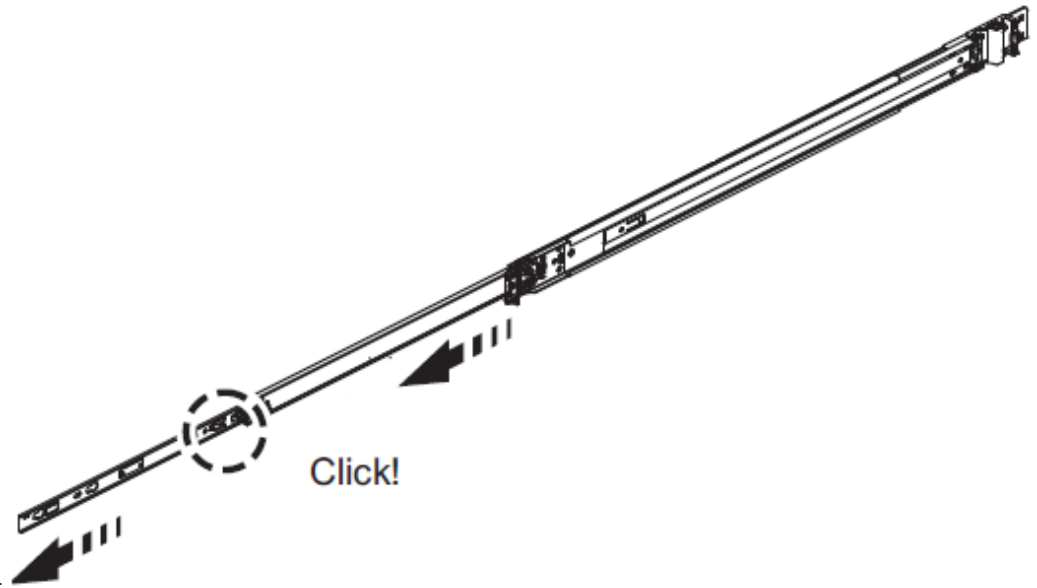
Follow this procedure to assemble the slide rails and position the Sensor on it.

#### Note

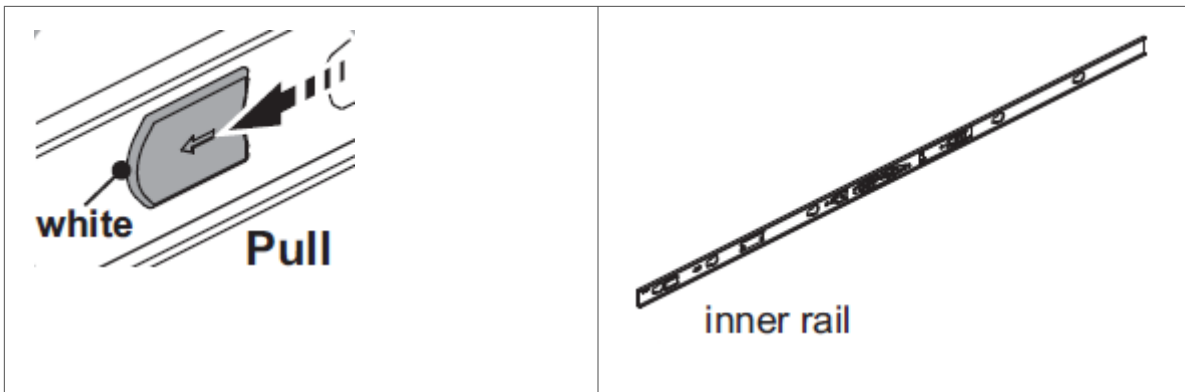
Due to the weight of the appliance, Trellix recommends that two people place the chassis into the rail cabinet.

1. Disassemble the inner slide rails from the rail assemblies.



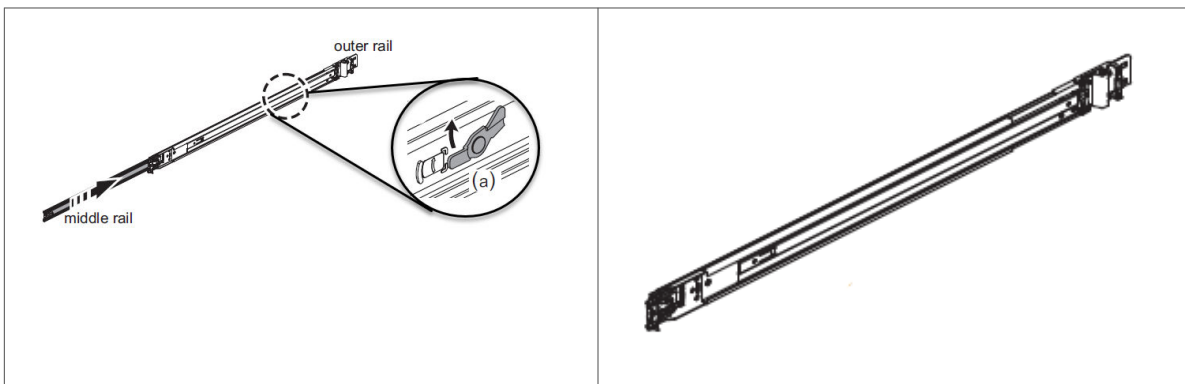


- a. Pull the inner rail out.
- b. Click and pull the white tab (lock on inner rail) forward to disconnect inner rail from the middle rail.



The Inner rail is disconnected.

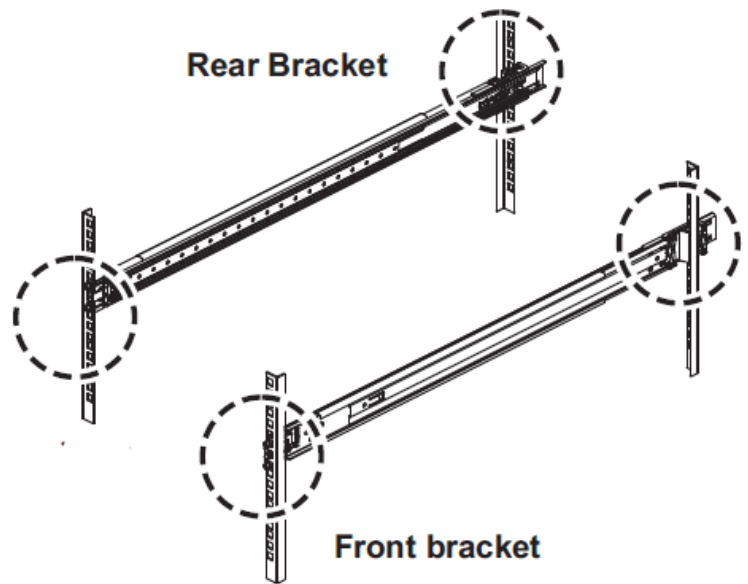
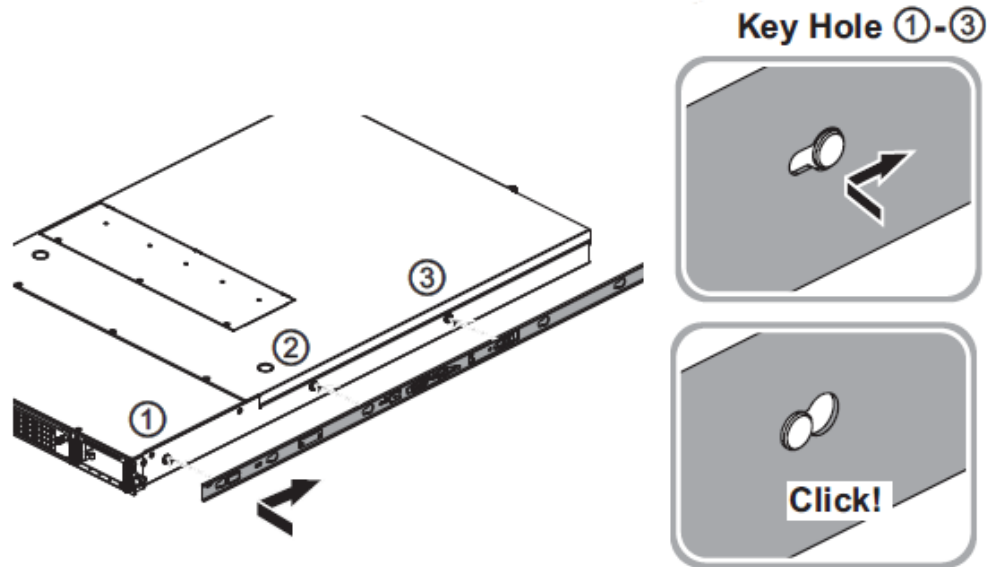
- c. Push tab (a) to slide the middle rail back into the outer rail.



The middle rail is pushed back into the outer rail.

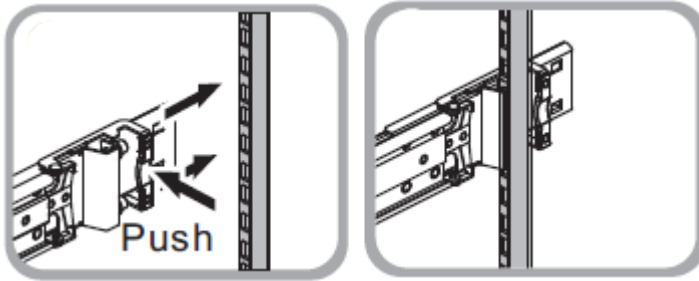
2. Mount the inner rail onto the chassis unit.

- 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.



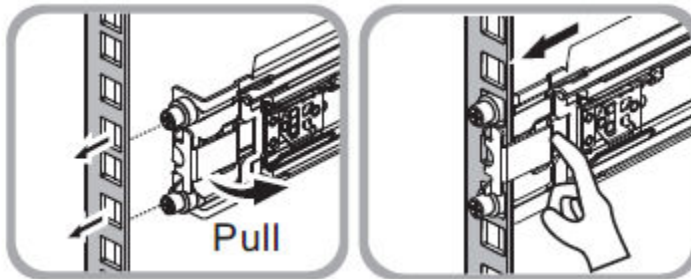
3. Mount the outer slide rails/brackets to the rack posts.

- 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



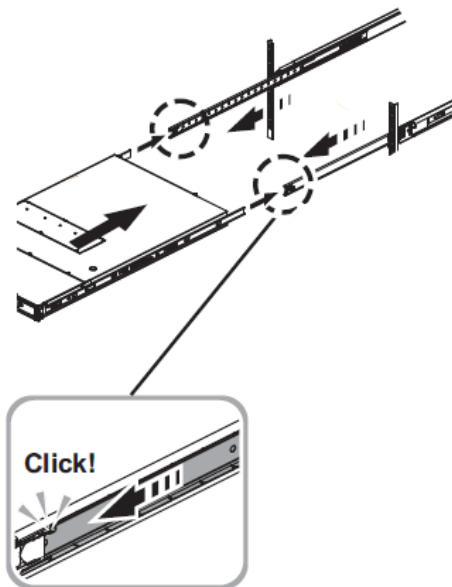
the securing latch onto the rack post.

- 4. Mount the chassis unit into the rack.

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

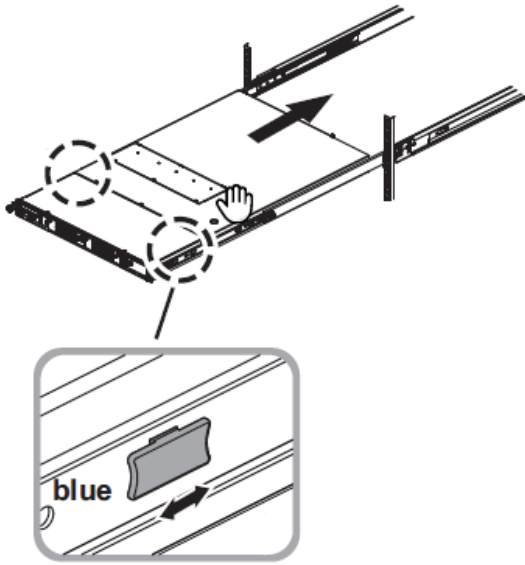
 **Note**

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

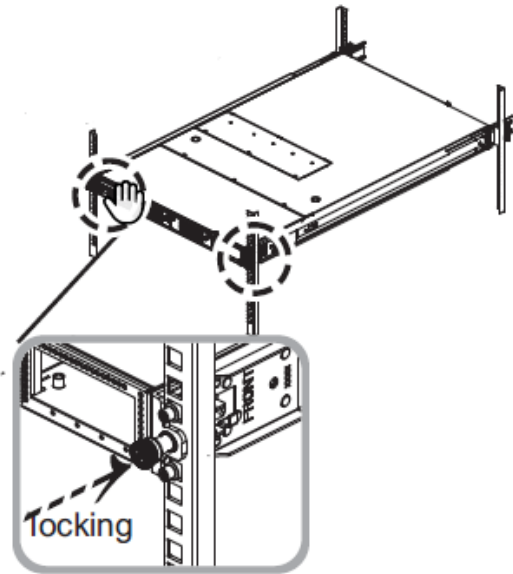


- b. Insert the chassis unit into the middle rails.

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.



:

## Redundant power supply

The basic configuration of a Sensor includes two hot-swappable power supplies. Each of these modules has one handle for insertion or extraction from the unit as well as a release latch. If you have purchased an additional power supply from Trellix, refer to the following sections to remove and install the new power supply.

---

Power supply unit



:

## Install a new power supply

### Steps:

1. Unpack the power supply from its shipping carton.
2. Remove the faceplate panel covering the power supply slot.

#### Note

The faceplate panel must remain in place unless a power supply is in the power supply slot. Do not operate the Sensor without the faceplate panel in place.

3. Place the power supply in the slot with the cable outlet facing front and on the left side of the faceplate.
4. Slide in the power supply until it makes contact with the backplane, then push firmly to mate the connectors solidly with the backplane.

#### Note

For true redundant operation with the power supply, Trellix recommends that you plug each supply into a different power circuit. For optimal protection, use uninterruptible power sources.

:

## Remove the power supply

Perform this task if you want to remove the power supply to the Sensor.

### Steps:

1. Unplug the power cable from its power source and remove the power cable from the power supply.
2. Push the release latch sideways toward the handle.
3. Center the handle of the power supply and pull on it to remove the power supply.
4. Use faceplate panels to protect unused slots from dust and to reduce electromagnetic radiation.
5. Replace the mounting bracket.

### Caution

To avoid data interruption, do not turn off both power supplies on an in-line Sensor; or else the Sensor shuts down and all Sensor function stops. Turn off only the power supply that you are replacing.

### Note

To remove all power from the Sensor, unplug all power cords.

:

## NS7x50 Network Interface modules

The NS7x50 Sensors support the 4-port, 6-port, and 8-port Network Interface modules. These modules need to be installed in the respective slots on the Sensor. The supported modules are the following:

- 4-port 10/1 Gig SM 8.5 micron with internal fail-open interface module
- 4-port 10/1 Gig MM 50 micron with internal fail-open interface module
- 4-port 10/1 Gig MM 62.5 micron with internal fail-open interface module
- 4-port RJ-45 10 Gbps/1 Gbps/100 Mbps with internal fail-open interface module
- 6-port RJ-45 10/100/1000 Mbps with internal fail-open interface module
- 8-port SFP/SFP+ 1/10 Gigabit interface module

For more information, refer to the *NS-series Interface Modules* section in *Trellix Intrusion Prevention System NS-series Reference Guide*.

:

## Installation of the Interface Module

This section provides instructions on how to install the interface module based on the following scenarios:

- Install the interface module during a fresh installation of the Sensor.
- Install the interface module on an up and running Sensor.

:

## Install the interface module during a fresh installation of the Sensor

This section provides the steps to install the interface module for a fresh installation of Manager and Sensor.

### Steps:

1. Remove the module from its protective packaging.

#### Note

It is assumed that the Sensor is yet to be powered on, and trust between the Sensor and the Manager has not been established.

2. Grip the sides of the module with your thumb and forefinger and insert the module into the slot.

---

#### Install an interface module



3. Drive in the screws fixed on the sides of the module to attach it to the Sensor.
4. Turn on the Sensor.
5. Establish trust between the Sensor and the Manager.

:

## Install the interface module on an up and running Sensor

This section provides the steps to install the interface module on a Sensor which is up and running.

**Steps:**

1. Power on the Sensor without inserting the pluggable module(s) into the slot(s).
2. Establish trust between the Sensor and the Manager.
3. Grip the sides of the module with your thumb and forefinger and insert the module into the slot.
4. Wait for 5 minutes.
5. Reboot the Sensor from the CLI.

:

**Remove an Interface Module**

Perform these steps if you need to remove an interface module.

1. Disconnect the network fiber optic cable from the module.
2. Remove the transceivers from the module.
3. Unscrew the interface modules to detach them from the Sensor.
4. Place the module into its protective packaging.

:

**Small form-factor pluggable transceiver modules**

The NS7x50 Sensors use two types of small form-factor pluggable transceiver modules as shown in the following table. For more information, see the *NS-series Transceiver Modules* section in *Trellix Intrusion Prevention System NS-series Reference Guide*.

Type	Performance
SFP	1 Gbps (copper) 1 Gbps (fiber optic)
SFP+	10 Gbps (fiber optic)

Each module is a hot-swappable input/output device that plugs into an LC-type Gigabit Ethernet port, linking the module port with a copper or fiber-optic network. SFP optical interfaces are less than half the size of GBIC interfaces.

To ensure compatibility, Trellix supports only those SFP, SFP+, QSFP+ and QSFP28 modules purchased through Trellix or from a Trellix-approved vendor. For a list of approved vendors, locate the relevant KnowledgeBase article at <https://supportm.trellix.com>. Enter the relevant KnowledgeBase article in Search the Support Knowledge Center and click Search to locate the article.



These installation instructions provide information for installing SFP and SFP+ modules that use a bail clasp for securing the module in place in the Sensor. Your module might be slightly different. Check the module manufacturer's installation instructions for more details. For ease of installation, insert the module in the Sensor while it is turned off and before placing it on a rack.

### Caution

To prevent eye damage, do not stare into open laser apertures.

:

## Install a transceiver module

### Steps:

1. Remove the module from its protective packaging.
2. Locate the label on the module and make sure that the alignment groove is down.
3. Grip the sides of the module with your thumb and forefinger and insert the module into the module socket. Modules are keyed to prevent incorrect insertion.

---

Insert a transceiver module



:

## Remove a transceiver module

Perform these tasks if you need to remove a module.

### Steps:

1. Disconnect the network fiber-optic cable from the module.
2. Release the module from the slot by pulling the bail clasp out of its locked position.
3. Slide the module out of the slot.
4. Insert the module plug into the module optical bore for protection.

:

## Attaching cables to the Sensor

Follow the steps outlined in this chapter to connect the cables to the various ports of your Sensor.

:

### Connect the cable to the Console port

The Console port on the NS7x50 Sensor is used for setup and configuration of the Sensor.

#### Steps:

1. For console connections, plug the DB9 Console cable supplied by Trellix into the Console port on the Sensor. This port is labeled **Console** in the Sensor front panel.



2. Connect the other end of the Console port cable directly to a COM port of the computer or terminal server you will use to configure the Sensor, for example, a computer 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. Required settings for HyperTerminal are listed below:

Name	Setting
Baud rate	115200
Number of bits	8
Parity	None
Stop bits	1
Flow control	None

3. Turn on the Sensor.

:

### Connect the cable to the Response port

When operating in tap or SPAN mode, the Sensor uses its Response port to respond to attacks. When deployed in tap mode, the Sensor does not inject response packets through the tap but uses the Response port.

#### Steps:

1. Plug a Cat-5e Ethernet cable into the Response port. This port is labeled **R1** on the Sensor rear panel.
2. Connect the other end of the cable to the network device, such as a hub, switch, or a router, through which you want to respond to attacks.

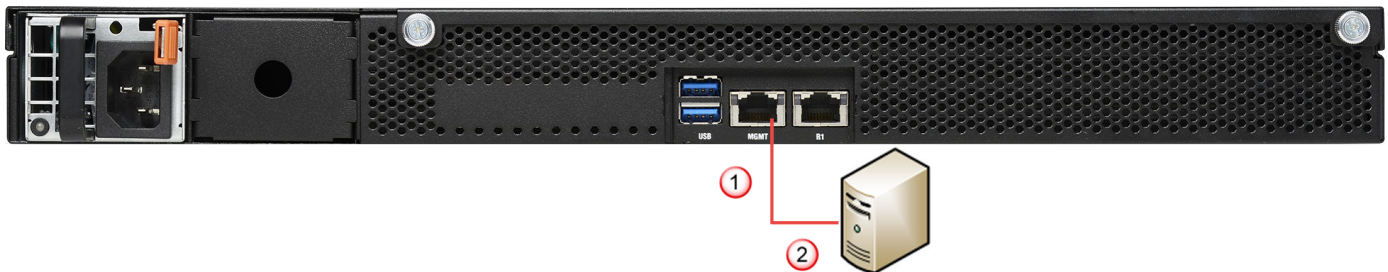
:

### Connect the cable to the Management port

The Sensor communicates with the Manager using the Management port.

#### Steps:

1. Plug a Category 5e Ethernet cable into the Management port. This port is labeled **Mgmt** in the rear panel of the NS7x50 Sensor.



2. Plug the other end of the cable into the network device connected to your Manager server.

#### Note

To isolate and protect your management traffic, Trellix strongly recommends you to use a separate, dedicated management subnet to interconnect the Sensors and the Manager.

:

### About connecting cables to the Monitoring ports

Connect to the network devices that you want to monitor through the Sensor monitoring ports. You can deploy Sensors in the following operating modes:

- In-line mode (fail-close)
- In-line mode (fail-open)
- External tap mode
- SPAN or hub mode

:

## How to use peer ports

You must use two peer Monitoring ports of the Sensor to deploy it full duplex mode. On the Sensor, the numbered ports are wired in pairs to accommodate the traffic.

### Note

- On NS7150, NS7250 and NS7350 Sensors, G0 and G3 indicate the fixed port slots. G1 and G2 indicate the slots for interface modules.
- In the following table, it is assumed that G1 is a 6-port RJ-45 1 Gbps/100 Mbps/10 Mbps interface module and G2 is the 8-Port SFP+/SFP 1/10G interface module. These interface modules can be interchanged.
- Since monitoring ports are internally wired, when you disable one of the ports in a pair, the corresponding port is also disabled.

The following Ethernet ports are coupled and must be used together. The number of ports for G2 and G3 are only illustrative since the actual number of port pairs can vary depending on the interface module that you use.

Port Pairs	Sensor
G0/1 and G0/2	NS7350/NS7250/NS7150
G1/1 and G1/2	NS7350/NS7250/NS7150
G1/3 and G1/4	NS7350/NS7250/NS7150
G1/5 and G1/6	NS7350/NS7250/NS7150
G2/1 and G2/2	NS7350/NS7250/NS7150
G2/3 and G2/4	NS7350/NS7250/NS7150
G2/5 and G2/6	NS7350/NS7250/NS7150

Port Pairs	Sensor
G2/7 and G2/8	NS7350/NS7250/NS7150
G3/1 and G3/2	NS7350/NS7250/NS7150
G3/3 and G3/4	NS7350/NS7250/NS7150
G3/5 and G3/6	NS7350/NS7250/NS7150
G3/7 and G3/8	NS7350/NS7250/NS7150

:

## Cable types for routers, switches, hubs, and computers

This section lists the types of cables that you require to connect the Sensor to other network devices:

- Use a crossover Ethernet RJ-45 cable to connect a router port to the SFP/SFP+ monitoring ports.
- Use a straight-through Ethernet RJ-45 cable to connect a switch or a hub port to SFP/SFP+ monitoring ports.
- Use a crossover Ethernet RJ-45 cable to connect a router port to computer to the Sensor Management port.
- Use a crossover Ethernet RJ-45 cable to connect a computer to the Sensor monitoring port.

:

## Connect the cables for in-line mode

In-line Gigabit Ethernet ports can be configured as fail-open or fail-closed. The RJ-45 monitoring ports are built-in and include an built-in fail-open functionality as well.

All other monitoring ports require the use of external active fail-open (AFO) kits for In-Line Fail-Open Active configuration.

Gigabit Ethernet ports fail-close, means the flow of traffic will stop if the Sensor fails. To allow traffic to flow uninterrupted, you must use special hardware, and cable the Sensor to external active fail-open kits. For instructions, see the subsequent sections of this chapter.

This section provides the steps to connect the Sensor's Gigabit Ethernet ports so they fail-close.

1. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports, for example G1/1.

2. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports, for example G1/2.



3. 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).

:

## Connect the cables for tap mode

To deploy the Sensor in tap mode, you must use a Sensor's Gigabit Ethernet Monitoring port pair with a third-party external tap.

### Note

For a list of Trellix-approved third party vendors, see the KnowledgeBase at <https://supportm.trellix.com>. Enter the relevant KnowledgeBase article in Search the Support Knowledge Center and click Search to locate the relevant KnowledgeBase article.

### Steps:

1. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports, for example, G1/1.
2. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports labeled G1/2.
3. Connect the other end of each cable to the tap.
4. Connect the network devices that you want to monitor to the tap.

:

## Connect the cables for SPAN or hub mode

For the Sensor, monitoring in SPAN or hub mode occurs in in-line fail-open mode. When you monitor in SPAN or hub mode, you use only single ports.

To connect an Sensor to a SPAN port or hub, plug an LC fiber-optic or 45 cable into one of the modules and connect the other end of the cable to the SPAN port or the hub.

:

## Connect the cables for Sensor Fail-Open

The Fail-Open Kits minimize the potential risks of in-line Sensor failure on critical network links. You need to purchase these kits separately. Both copper and optical versions of the kit are available for the one-gigabit ports. The standard Gigabit Fail-Open Kits and 10 Gigabit Fail-Open Kits are available for the 1 and 10 gigabit ports respectively.

The Monitoring ports of the Sensors can be fail-close; thus, if the Sensor is deployed in-line fail-close, a hardware failure results in network downtime. Except the built-in RJ-45 ports which come with built-in fail-open functionality, you use the optional external bypass switch provided in an Active Fail-Open Kit for the Monitoring ports to fail-open.

While the Sensor is operating, the Active Fail-Open (AFO) kit is in-line and routes all traffic directly through the Sensor. When the Sensor fails, the switch automatically shifts to a bypass state; in-line traffic continues to flow through the network link but is no longer routed through the Sensor. After the Sensor resumes normal operation, the switch returns to the "inline" state, once again enabling in-line monitoring. The port pairs with AFO kits resume inline mode after a Sensor resumes normal operation or is in good health.

- G0 supports passive fail-open mode with RJ-11 port control

### Note

G0 also supports active fail-open using a Copper and Fiber 1/10 Gigabit AFO kit.

- G1 and G2 supports built-in fail-open and active fail-open mode for these interface modules:
  - 4-port 10 GigE/1 GigE LR Optical with internal fail-open
  - 4-port 10 GigE/1 GigE SR Optical 50 micron with internal fail-open
  - 4-port 10 GigE/1 GigE SR Optical 62.5 micron with internal fail-open
  - 4-port RJ-45 10 GigE with internal fail-open
  - 6-port RJ-45 1 GigE with internal fail-open

### Note

All RJ-45 ports support active fail-open using only a Copper AFO kit.

- 8-port SFP/SFP+ 1/10 Gigabit

### Note

The 8-port module supports active fail-open using a Copper and Fiber 1/10 Gigabit AFO kit.

- G3 supports both internal fail-open and active fail-open mode when connected to an Active Fail-Open (AFO) kit

 **Caution**

Sensor outage breaks the link connecting the devices on either side of the Sensor for a brief moment and requires the renegotiation of the network link between the two peer devices connected to the Sensor. Depending on the network equipment, this disruption introduced by the renegotiation of the link layer between the two peer devices might range from a couple of seconds to more than a minute with certain vendors' devices.

 **Caution**

A very brief link disruption might also occur while the links between the Sensor and each of the peer devices are renegotiated to place the Sensor back in in-line mode. This outage, again, varies depending on the device, and can range from a few seconds to more than a minute. The performance of the switchover from in-line to bypass and vice versa varies depending on the vendor.

You can find the installation and troubleshooting instructions for the kit in the guide that accompanies the kit. For example, for more information on the Optical kits, see the *1 Gigabit Optical Active Fail-Open Bypass Kit Guide* and *10 Gigabit Optical Active Fail-Open Bypass Kit Guide*.

:

## Connect the cable for Sensor failover

For Sensor failover, connect two NS7x50 Sensors using the standard LC-LC cables. These two Sensors must be running the same software version.

Purchase two 10G SFP+ and use the standard cable. Failover cables are additional hardware required to support failover communication between two NS7x50 Sensors.

 **Note**

Trellix does not ship the transceiver modules and cables with the NS7x50 Sensors. Please purchase the same separately for failover setup.

Refer to the following table before you configure a HA pair:

Sensor Model	Port to connect the HA pair	Cable requirements for failover
NS7350/NS7250/NS7150	G0/1	2 10G SFP+ and standard LC-LC cable



**Steps:**

1. Plug the cable appropriate for use with your SFP+ module into port G0/1 of the active NS7x50 Sensor.
2. Connect the other end of the cable with SFP+ into port G0/1 of the standby NS7x50 Sensor.

:

**Turning the Sensor on and off** **Note**

Do not attempt to turn on the Sensor until you have installed the Sensor in a rack and made all the necessary network connections.

**Steps:**

1. Connect the power cable to the Sensor power inlet.
2. Connect the power cable to a power source.

 **Note**

If you are installing a redundant power supply, you should install it as described in *Install a new power supply* section. For true redundant operation with the power supply, Trellix recommends that you plug each supply into a different power circuit.

The Sensor has no power switch. The Sensor turns on as soon as one of its power cables is connected to a power source. Trellix recommends that you use the **shutdown** CLI command to halt the Sensor before turning it off. For more information on CLI commands, see *CLI commands* section in *Trellix Intrusion Prevention System Product Guide*.

:

**Troubleshooting the Sensor**

This section lists some common installation problems, the possible causes, and the corresponding solutions.

<b>Problem</b>	<b>Possible Cause</b>	<b>Solution</b>
LED is off.	The Sensor is turned off.	Restore Sensor power.

<b>Problem</b>	<b>Possible Cause</b>	<b>Solution</b>
LED is off.	The Sensor port cable is disconnected.	Check the Sensor cable connections.
Sensor is operational but is not monitoring traffic.	Network device cables have been disconnected.	Check the cables and make sure they are properly connected to both the network devices and the bypass switch.
Sensor is operational but is not monitoring traffic.	The Sensor ports have not been enabled in the Manager.	The Sensor will not monitor traffic on the ports unless the ports are enabled in the Manager. Ports are disabled in case of Sensor failure; you must re-enable them for Sensor monitoring to resume.
Network or link problems	Improper cabling or port configuration	Make sure that the transmitting and receiving cables are properly connected to the bypass switch.
Runts or giants errors on switch and routers	Improper cabling or port configuration	Make sure that the transmitting and receiving cables are properly connected to the bypass switch.
The system fault "Switch absent" appears in the Manager Status page.	The Active Fail-Open Kit is disconnected.	Check the Active Fail-Open Kit and make sure it is properly connected to the Sensor.

:

## Sensor technical specifications

The following table lists the specifications of an NS7x50 Sensor:

Sensor Specifics	NS7350	NS7250	NS7150
Dimensions	17.31" (W) x 1.75" (H) x 29.13" (D)	17.31" (W) x 1.75" (H) x 29.13" (D)	17.31" (W) x 1.75" (H) x 29.13" (D)
Weight	28 lbs	28 lbs	28 lbs
Storage	Solid State 240 GB	Solid State 240 GB	Solid State 240 GB
<b>System Heat Dissipation</b>			
Maximum BTU	1024 BTU/hr	1024 BTU/hr	1024 BTU/hr
Typical BTU	853 BTU/hr	853 BTU/hr	853 BTU/hr
Maximum Power Consumption	300 W	300 W	300 W
Redundant Power Supply	Included	Included	Included
Power	100-240V AC (50/60Hz)		
Temperature	Operating: 0°-35° C , Non-operating: -40°- 70° C		
Relative humidity (non-condensing)	Operational: 10% -90%, Non-operational: 5% -95%		
Altitude	0 to 10,000 feet		
Safety Certification	UL 60950-1 (USA); CSA 22.1.No. 60950-1 (Canada); EN 60950-1 (Europe); CNS 14336-1 (Taiwan), KN32 and KN35 (South Korea); GB 4943-1 and GB 17625.1 (China); IEC 60950-1 (International) - CB Scheme certificate and test report covering all applicable country deviations; IEC 60825 and 21CFR1040		
EMI Certification	FCC Part 15 Subpart B Class A (USA); CAN ICES-3 Class A (Canada); EN 55022, EN 55032, EN 55024, EN61000-3-2, EN61000-3-3 (Europe and International);		

Sensor Specifics	NS7350	NS7250	NS7150
	VCCI Class A (Japan); AS/NZS CISPR 32 (Australia and New Zealand); CNS 13438 (Taiwan); GB 9254-2008 (China)		

:

## NS7x00 Sensors

:

### About Sensors

Sensors are high-performance, scalable, and flexible content processing appliances built for accurate detection and prevention of:

- Network intrusions
- Network misuse
- Distributed Denial-of-Service (DDoS) attacks

Sensors are specifically designed to handle traffic at wire speed, efficiently inspect and detect intrusions with a high degree of accuracy, and are flexible enough to adapt to the security needs of any enterprise environment. When deployed at key network access points, the Sensor provides real-time traffic monitoring to detect malicious activity and respond to such activity based on the responses configured by the administrator.

After you deploy a Sensor successfully, you configure and manage it using the Manager. The process of configuring a Sensor and establishing communication with the Manager is described in the subsequent chapters of this guide. For details about the Manager, see the *Manager Administration* section in *Trellix Intrusion Prevention System Product Guide*.

:

### Functions of an NS-series Sensor

The NS-series Sensors are a third-generation hardware platform for Sensors designed for high bandwidth links to offer Next Generation IPS (NGIPS) capability and provide high aggregate throughput across various Sensor models. The following models are supported.

- NS7300 - The NS7300 Sensor is a 1RU unit, providing an aggregate throughput of 5 Gbps
- NS7200 - The NS7200 Sensor is a 1RU unit providing an aggregate throughput of 3 Gbps
- NS7100 - The NS7100 Sensor is a 1RU unit providing an aggregate throughput of 1.5 Gbps

The primary function of a Sensor is to analyze traffic on selected network segments and to respond when an attack is detected. The Sensor examines the header and data portion of every network packet, looking for patterns and behavior in the network traffic that indicate malicious activity. The Sensor examines packets according to user-configured policies, or rule sets, which determine what attacks to watch for, and how to respond with countermeasures if an attack is detected.

If an attack is detected, a Sensor responds according to its configured policy. Sensor can perform many types of attack responses, including generating alerts and packet logs, resetting TCP connections, "scrubbing" malicious packets, and even blocking attack packets entirely before they reach the intended target.

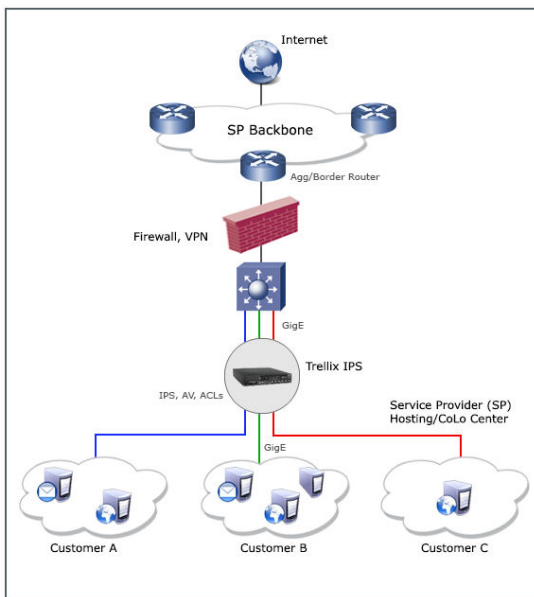
:

## Deployment of an NS-series Sensor

Deployment of a Sensor requires knowledge of your network to help determine the level of configuration and the number of installed Sensors. You also need to determine the number of Trellix ePolicy Orchestrator - On-prem servers required to protect your network. The Sensor is purpose-built for the monitoring of traffic across one or more network segments.

Following is an example of a network topology using Gigabit Ethernet throughput. In the illustration, Trellix Intrusion Prevention System provides IPS protection to outsourced servers. High port-density and virtualization provides a highly scalable solution, while Trellix IPS protects against web and eCommerce mail server exploits.

### A sample NS-Series Sensor deployment



:

## NS7x00 Sensor physical description

The high-port density NS-series Sensor is designed for high bandwidth links. This section gives a physical description of the NS7x00 Sensors.

The NS7300, NS7200, and NS7100 Sensor models are a mid-range offering that provide 5 Gbps, 3 Gbps, and 1.5 Gbps throughput respectively.

:

## Components of an NS7x00 Sensor

The NS7x00 front and rear panel details are described below.

## The NS7100/NS7200/NS7300 Sensor model

### Sensor front panel



1. Console port (1)
2. RJ-11 port (1) for fail-open control of two built-in SFP+ ports in slot G0. The RJ-11 port supports 1 Gbps (SFP) copper or fiber and 10 Gbps (SFP+) (SR and LR)
3. SFP+ 1/10 Gigabit Ethernet ports (2)

### **i** Important

The RJ-11 port controls only this SFP+ 1/10 port pair in passive fail-open mode.

4. Two slots for I/O modules (Any combination of the interface modules can be used)
  - SFP/SFP+ 1/10 Gigabit Ethernet Monitoring ports (8)
  - RJ-45 10/100/1000 Mbps with internal fail-open Ethernet Monitoring ports (6)
  - 10/1 GigE SM 8.5 micron with internal fail-open Monitoring ports (4)
  - 10/1 GigE MM 50 micron with internal fail-open Monitoring ports (4)
  - 10/1 GigE MM 62.5 micron with internal fail-open Monitoring ports (4)
5. RJ-45 10/100/1000 Mbps Ethernet Monitoring ports (8)

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

### Sensor rear panel



1. Auxiliary port (1)
2. USB ports (2)
3. Power supply inlet (2)
4. RJ-45 10/100/1000 Response port (R1) (1)
5. RJ-45 10/100/1000 Management port (Mgmt) (1)

The NS7x00 Sensors have five fan units on the top.

Fan units-NS7100/NS7200/NS7300



The direction of airflow in all the Sensors is front to back. Cold air enters through the front of the chassis.

**Note**

The fan units and power supplies are field replaceable.

The following table gives the details of the supported ports.

Ports	NS7100/NS7200/NS7300
Fixed Gigabit Ethernet—Copper ports (internal fail-open)	8
Fixed 10 GigE/1 GigE (SFP+) ports	2
Network I/O slots	2
Network I/O modules	4-port 10/1 GigE SM 8.5 micron with internal fail-open



Ports	NS7100/NS7200/NS7300
	4-port 10/1 GigE MM 50 micron with internal fail-open 4-port 10/1 GigE MM 62.5 micron with internal fail-open 6-port RJ-45 1 GigE with internal fail-open 8-port (SFP+/SFP) 10/1 GigE
10 Gigabit Ethernet	Modular up to 18
Dedicated Response ports (RJ-45)	1 (1G/100M/10M)
Dedicated Management ports (RJ-45)	1 (1G/100M/10M)
Dedicated Auxiliary port (DB9)	1
USB ports	2

- **Console port** — Use to set up and configure the Sensor using the CLI.
- **RJ-11 port** — Controls the SFP+ 1/10 Gigabit Ethernet port pair in passive fail-open mode
- **SFP/SFP+ 1/10 Gigabit Ethernet ports** — Enables to monitor two SPAN ports, two segments in-line, or a combination
- **RJ-45 10/100/1000 Mbps Ethernet Monitoring ports** — Enables to monitor eight SPAN ports, four segments in-line, or a combination
- **DB9 Auxiliary port** — Use to dial in remotely to set up and configure the Sensor.
- **External USB ports** — Use these in troubleshooting situations for system recovery purposes. You need to restart the Sensor through the USB storage device.
- **RJ-45 10/100/1000 Management port**— Use for communication with the Manager server. You can assign an IP address to this port during installation.
- **RJ-45 10/100/1000 Response port** — When you're operating in SPAN or tap mode, enables you to inject response packets back through a switch or router.
- **Power Supply** — Power supply is included with an NS7x00 Sensor. The supply uses a standard IEC port (IEC320-C13). Trellix provides a standard, 2m NEMA 5-15P (US) power cable (3 wire). International customers must procure a country-appropriate power cable.

The NS-series Sensor does not have internal taps; you must use it with a third-party external tap to run it in tapped mode.

:

## Sensor LEDs

The front and rear panel LEDs provide status information for the health of the Sensor and the activity on its ports. The following table describes the NS-series LEDs.

### Front panel LEDs

LED	Status	Description
Status	Green Amber	Sensor is operating in good health. it also indicates system bad health. Sensor is booting up. (It could also indicate a system failure.)
Fan	Green Amber	All the fans are operating. One or more fans are not working.
Temp	Green Amber	Inlet air temperature measured inside the chassis is normal. (Chassis temperature OK) Inlet air temperature measured inside the chassis is too high. (Chassis temperature too hot)
Gigabit Ports Act	Blinking Amber Off	Data is received or transmitted. No data is being transferred.
Gigabit Ports Link	Green Off	The link is up. The link is down.
Normal/Bypass	Green Off	The port pair is in Inline Fail-Open/Inline Fail-Close/SPAN/Tap Mode. The Port Pair is in the Bypass Mode.

## Rear panel LEDs

LED	Status	Description
Power	Solid Green Blinking Green Solid Amber	Power supply has power feed and is functioning. Power Supply is stand-by. It also indicates load sharing. Power Supply is not functioning or the unit has no power feed.
Management Port Speed	Green Amber Off	The port speed is 1000 Mbps. The port speed is 100 Mbps. The port speed is 10 Mbps.
Management Port Link	Green Off	The link is up. The link is down.
Response Port Speed	Green Amber Off	The port speed is 1000 Mbps. The port speed is 100 Mbps. The port speed is 10 Mbps.
Response Port Link	Green Off	The link is up. The link is down.

:

## Before you install

This chapter describes the best practices for deployment of Sensors in your network. Topics include the safety considerations for handling the Sensor, usage restrictions that apply to the Sensor model, and the contents that are shipped along with the Sensor.

:

### Usage restrictions

The following restrictions apply to the use and operation of a Sensor:

- You should not remove the outer shell of the Sensor. If you do so, this will invalidate your warranty.

- The Sensor appliance is not a general purpose workstation.
- Trellix prohibits the use of the Sensor appliance for anything other than operating Trellix IPS.
- Trellix prohibits the modification or installation of any hardware or software on the Sensor appliance that is not part of the normal operation of Trellix IPS.

:

### Safety measures

Please read the following warnings before you install the Sensor. These safety measures apply to all Sensor models unless otherwise noted. Failure to observe these safety warnings could result in serious physical injury.

#### Warnings:

- Read the installation instructions before you connect the system to its power source.
- To remove all power from the Sensor, unplug all power cords, including the redundant power cord.
- Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
- Before working on the equipment that is connected to power lines, remove all jewelry including rings, necklaces, and watches. Metal objects will heat up when connected to power and ground, and can cause serious burns or weld the metal object to the terminals.
- This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.
- Do not remove the outer shell of the Sensor. Doing so will invalidate your warranty.
- Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Blank faceplates and cover panels prevent exposure to hazardous voltages and currents inside the chassis, contain electromagnetic interference (EMI) that might disrupt other equipment and direct the flow of cooling air through the chassis.
- To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the users will be required to correct the interference at their own expense.
- Refer to the Appendix for information on regulatory, compliance, and other safety requirements.

:

### About fiber-optic ports

The Sensor uses fiber-optic connectors for its Monitoring ports. The connector type is an SFP/SFP+ fiber optic connector that is LC-duplex compatible.

Note the following:

- Fiber-optic ports (for example, SFP/SFP+, FDDI, OC-3, OC-12, OC-48, ATM, GBIC, and 100BaseFX) are considered Class 1 laser or Class 1 LED ports.
- These products have been tested and found to comply with Class 1 limits of IEC 60825-1, IEC 60825-2, EN 60825-1, EN 60825-2, and 21CFR1040.

### Caution

To avoid exposure to radiation, do not stare into the aperture of a fiber-optic port. Invisible radiation could be emitted from the aperture of the port when no fiber cable is connected.

- Only FDA registered, EN 60825-1 and IEC 60825-1 certified Class 1 SFP/SFP+/ laser transceivers are acceptable for use with the Sensor.

:

## Contents of 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

:

## Unpack the Sensor

Steps:

1. Open the crate.
2. Remove the first accessory box.
3. Verify you have received all parts. These parts are listed on the packing list and in the *Contents of the box* section.
4. Remove the Sensor.
5. Place the Sensor box as close to the installation site as possible.
6. Position the box with the text upright.
7. Open the top flaps of the box.
8. Remove the accessory box within the Sensor box.
9. Verify you have received all parts. These parts are listed on the packing list and in the *Contents of the box* section.
10. Remove the Slide Rail Kit.
11. Pull out the packing material surrounding the Sensor.
12. Remove the Sensor from the antistatic bag.
13. Save the box and packing materials for later use in case you need to move or ship the Sensor.

:

## Setting up the Sensor

This chapter describes how to set up the Sensor for you to configure it.

:

### Setup overview

Setting up a Sensor involves these steps:

1. Position the Sensor.
2. Install interface modules (SFP and SFP+).
3. Attach power, network, and monitoring cables.
4. Turn on the Sensor.
5. Configure the Sensor after you have set up and turned it on.

:

### How to position the Sensor

Place the Sensor in a physically secure location, close to the switches or routers it will be monitoring. Ideally, the Sensor should be located within a standard communications rack. To mount the Sensor on a rack, you will attach two mounting rails to the Sensor as described in the subsequent sections of this guide.

:

### Install the slide rails and rack-mount the Sensor

Trellix recommends rack-mounting your Sensor. For maintenance purposes, you must have access to the front and rear of the Sensor.

#### Caution

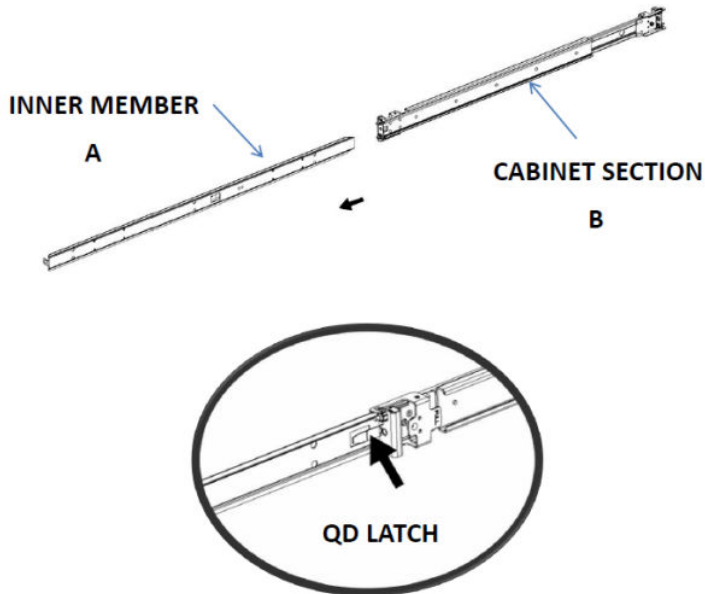
Before you mount the Sensor on the rack, make sure that the power is off. Remove the power cable and all network interface cables from the Sensor.

#### Note

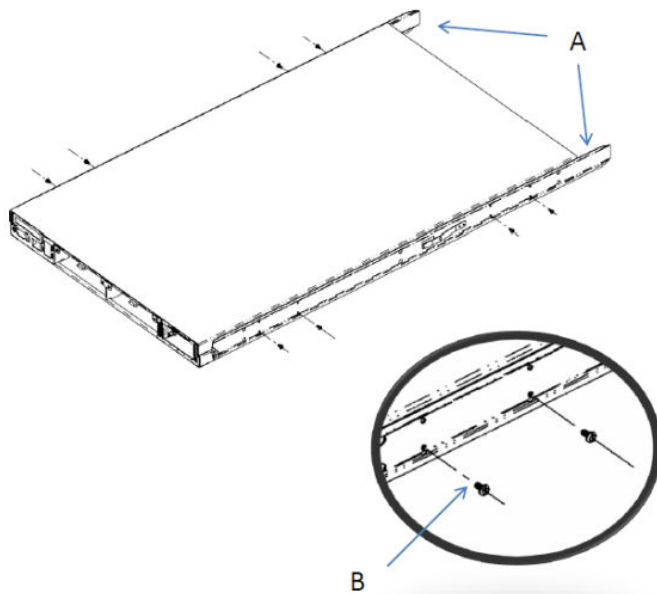
Due to the weight of the appliance, Trellix recommends that two people place the chassis into the rail cabinet.

1. Disassemble the inner slide rail members from the cabinet sections.

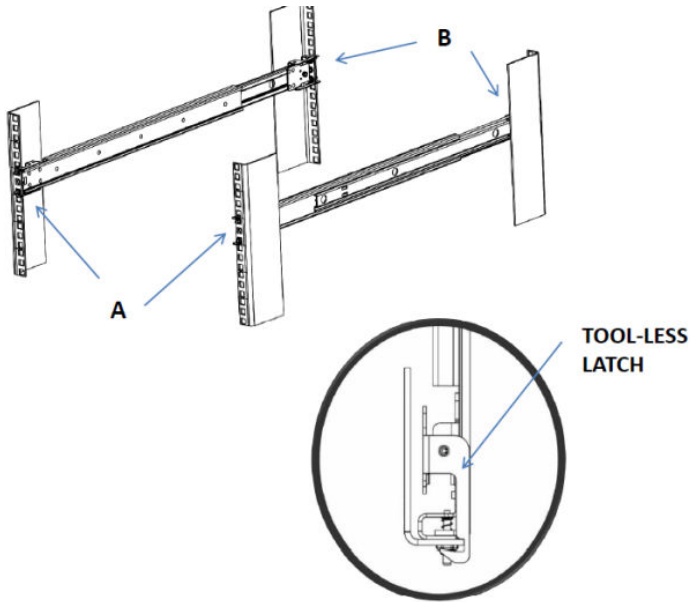
- a. Pull the inner member out until it comes to a lock position.
- b. Depress the QD latch to fully disconnect the inner members.



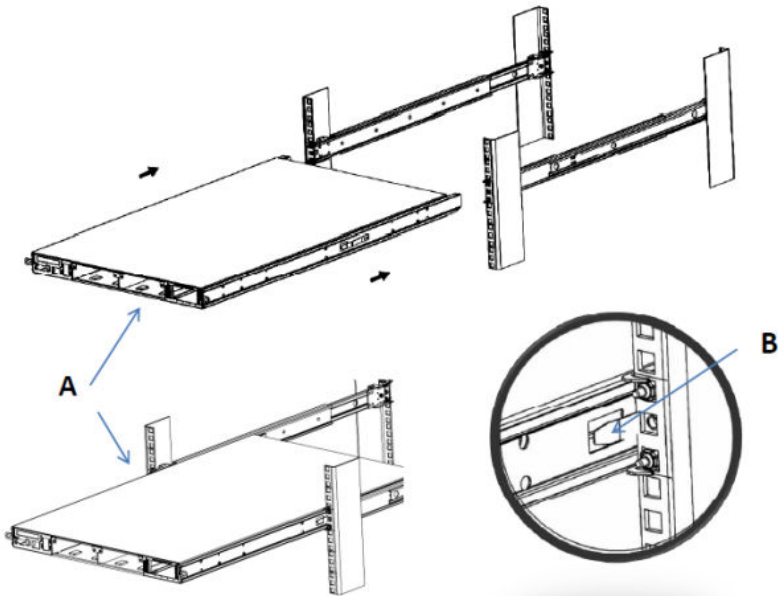
2. Mount the inner members to the chassis unit.
  - a. Place each inner member on both sides of the chassis unit. Position the bottom mounting holes of the inner member with matching mounting holes on chassis unit.
  - b. Use screws to secure inner members in place. Apply to both sides of chassis unit.



3. Mount the slide cabinet sections to the rack.
  - a. Install the front end of each slide cabinet section to the rack using the slide tool-less features. The tool-less latch rotates when the bracket is pressed up against the rack rails.
  - b. Align, adjust, and attach the rear brackets to the rack rail.

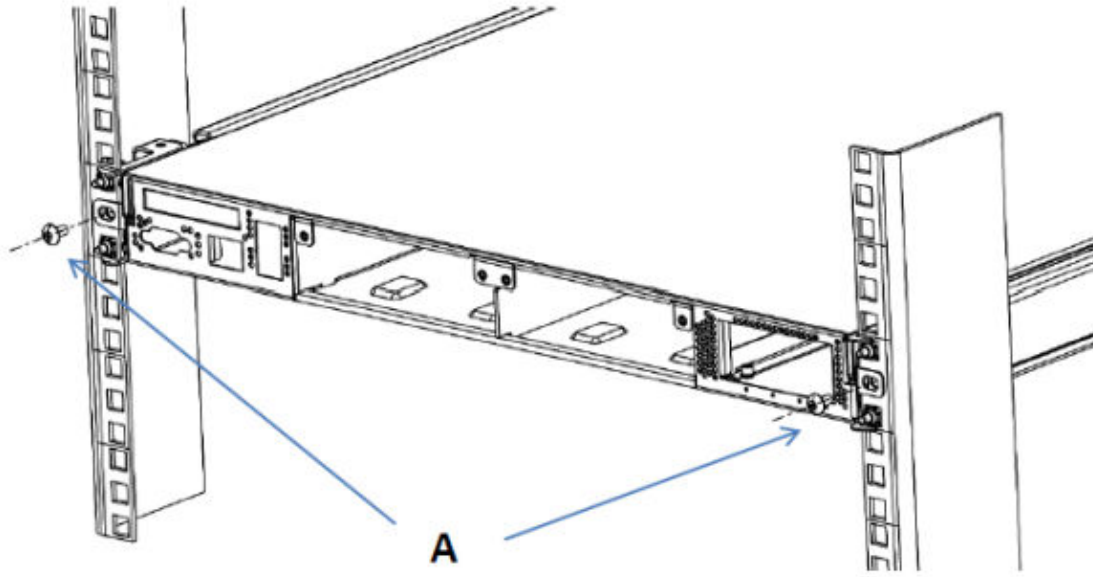


4. Mount the chassis unit into the mounted cabinet sections.
  - a. Guide the chassis unit into the pre-installed cabinet sections. Allow the pre-installed inner members to slide into the outer members until they lock in place.
  - b. Depress the QD latch on both sides and continue to push the chassis unit in until fully closed.



5. Secure the chassis unit through the rack rails.
  - a. With the chassis unit in a fully closed position, secure using two truss head screws.
  - b. Drive the screws through the inner member flange and through the rack rails. The screws thread directly to the cabinet slide members. Tighten the screws.





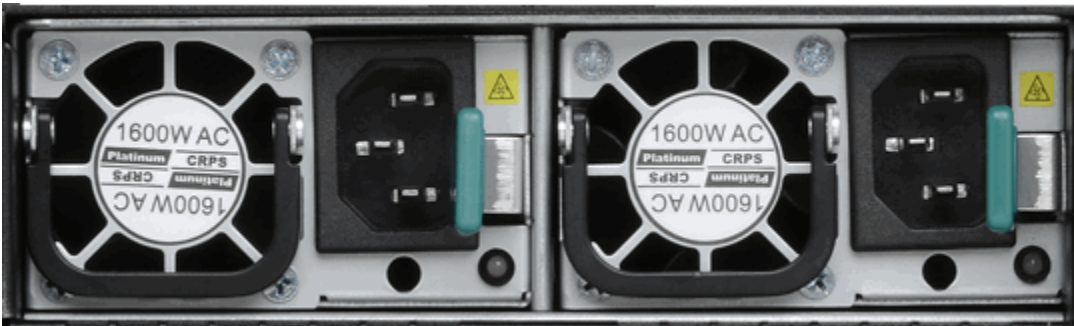
:

### Redundant power supply

A basic configuration of the Sensor includes one hot-swappable power supply. You can install a second hot-swappable power supply for redundancy. You will have to purchase this redundant power supply separately from Trellix. Each of these modules have one handle for insertion or extraction from the unit as well as a release latch.

---

#### Power supply units




:

### Install a new power supply

#### Steps:

1. Unpack the power supply from its shipping carton.
2. Remove the faceplate panel covering the power supply slot.

 **Note**

The faceplate panel must remain in place unless a power supply is in the power supply slot. Do not operate the Sensor without the faceplate panel in place.

3. Place the power supply in the slot with the cable outlet facing front and on the left side of the faceplate.
4. Slide in the power supply until it makes contact with the backplane, then push firmly to mate the connectors solidly with the backplane.

 **Note**

For true redundant operation with the optional redundant power supply, Trellix recommends that you plug each supply into a different power circuit. For optimal protection, use uninterruptible power sources.

:

## Remove the power supply

Perform this task if you want to remove the power supply to the Sensor.

### Steps:

1. Unplug the power cable from its power source and remove the power cable from the power supply.
2. Push the release latch sideways toward the handle.
3. Center the handle of the power supply and pull on it to remove the power supply.
4. Use faceplate panels to protect unused slots from dust and to reduce electromagnetic radiation.
5. Replace the mounting bracket.

 **Caution**

To avoid data interruption, do not turn off both power supplies on an in-line Sensor; or else the Sensor shuts down and all Sensor function stops. Turn off only the power supply that you are replacing.

 **Note**

To remove all power from the Sensor, unplug all power cords.

:

## NS7x00 Network Interface modules

The NS7x00 Sensors support the 4-port, 6-port, and 8-port Network Interface modules. These modules need to be installed in the respective slots on the Sensor. The supported modules are:

- 4-port 10/1 Gig SM 8.5 micron with internal fail-open interface module
- 4-port 10/1 Gig MM 50 micron with internal fail-open interface module
- 4-port 10/1 Gig MM 62.5 micron with internal fail-open interface module
- 6-port RJ-45 10/100/1000 Mbps with internal fail-open interface module
- 8-port SFP/SFP+ 1/10 Gigabit interface module

For more information, see the *NS-series Interface Modules* section in *Trellix Intrusion Prevention System NS-series Reference Guide*.

:

## Installation of the Interface Module

This section provides instructions on how to install the interface module based on the following scenarios:

- Install the interface module during a fresh installation of the Sensor.
- Install the interface module on an up and running Sensor.

:

### Install the interface module during a fresh installation of the Sensor

This section provides the steps to install the interface module for a fresh installation of Manager and Sensor.

Steps:

1. Remove the module from its protective packaging.

#### Note

It is assumed that the Sensor is yet to be powered on, and trust between the Sensor and the Manager has not been established.

2. Grip the sides of the module with your thumb and forefinger and insert the module into the slot.

---

Install an interface module



3. Drive in the screws fixed on the sides of the module to attach it to the Sensor.
4. Turn on the Sensor.
5. Establish trust between the Sensor and the Manager.

:

## Install the interface module on an up and running Sensor

This section provides the steps to install the interface module on a Sensor which is up and running.

### Steps:

1. Power on the Sensor without inserting the pluggable module(s) into the slot(s).
2. Establish trust between the Sensor and the Manager.
3. Grip the sides of the module with your thumb and forefinger and insert the module into the slot.
4. Wait for 5 minutes.
5. Reboot the Sensor from the CLI.

:

## Remove an Interface Module

Perform these steps if you need to remove an interface module.

1. Disconnect the network fiber optic cable from the module.
2. Remove the transceivers from the module.
3. Unscrew the interface modules to detach them from the Sensor.
4. Place the module into its protective packaging.

:

## Small form-factor pluggable transceiver modules

The NS7x00 Sensors use two types of small form-factor pluggable transceiver modules as shown in the following table. For more information, see the *NS-series Transceiver Modules* section in *Trellix Intrusion Prevention System NS-series Reference Guide*.

Type	Performance
SFP	1 Gbps (copper) 1 Gbps (fiber optic)
SFP+	10 Gbps (fiber optic)

Each module is an input/output device that plugs into an LC-type Gigabit Ethernet port, linking the module port with a copper or fiber-optic network. SFP optical interfaces are less than half the size of GBIC interfaces.

To ensure compatibility, Trellix supports only those SFP, SFP+, QSFP+ and QSFP28 modules purchased through Trellix or from a Trellix-approved vendor. For a list of approved vendors, locate the relevant KnowledgeBase article at <https://supportm.trellix.com>. Enter the relevant KnowledgeBase article in Search the Support Knowledge Center and click Search to locate the article.

These installation instructions provide information for installing SFP and SFP+ modules that use a bail clasp for securing the module in place in the Sensor. Your module might be slightly different. Check the module manufacturer's installation instructions for more details. For ease of installation, insert the module in the Sensor while it is turned off and before placing it on a rack.

### Caution

To prevent eye damage, do not stare into open laser apertures.

:

### Install a transceiver module

#### Steps:

1. Remove the module from its protective packaging.
2. Locate the label on the module and make sure that the alignment groove is down.
3. Grip the sides of the module with your thumb and forefinger and insert the module into the module socket. Modules are keyed to prevent incorrect insertion.

---

Insert a transceiver module



:

### Remove a transceiver module

Perform these tasks if you need to remove a module.

#### Steps:

1. Disconnect the network fiber-optic cable from the module.
2. Release the module from the slot by pulling the bail clasp out of its locked position.
3. Slide the module out of the slot.
4. Insert the module plug into the module optical bore for protection.

:

## Attaching cables to the Sensor

Follow the steps outlined in this chapter to connect the cables to the various ports of your Sensor.

:

### Connect the cable to the Console port

The Console port on the NS7x00 Sensor is used for setup and configuration of the Sensor.

#### Steps:

1. For console connections, plug the DB9 Console cable supplied by Trellix into the Console port on the Sensor. This port is labeled **Console** in the Sensor front panel.



2. Connect the other end of the Console port cable directly to a COM port of the computer or terminal server you will use to configure the Sensor, for example, a computer 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. Required settings for HyperTerminal are listed below:

Name	Setting
Baud rate	115200
Number of bits	8
Parity	None
Stop bits	1
Flow control	None

3. Turn on the Sensor.

:

### Connect the cable to the Response port

When operating in tap or SPAN mode, the Sensor uses its Response port to respond to attacks. When deployed in tap mode, the Sensor does not inject response packets through the tap but uses the Response port.

#### Steps:

1. Plug a Cat-5e Ethernet cable into the Response port. This port is labeled **R1** on the Sensor rear panel.
2. Connect the other end of the cable to the network device, such as a hub, switch, or a router, through which you want to respond to attacks.

:

## Connect the cable to the Management port

The Sensor communicates with the Manager using the Management port.

### Steps:

1. Plug a Category 5e Ethernet cable into the Management port. This port is labeled **Mgmt** in the rear panel of the NS7x00 Sensor.



2. Plug the other end of the cable into the network device connected to your Manager server.

### Note

To isolate and protect your management traffic, Trellix strongly recommends you to use a separate, dedicated management subnet to interconnect the Sensors and the Manager.

:

## About connecting cables to the Monitoring ports

Connect to the network devices that you want to monitor through the Sensor monitoring ports. You can deploy Sensors in the following operating modes:

- In-line mode (fail-close)
- In-line mode (fail-open)
- External tap mode
- SPAN or hub mode

:

## How to use peer ports

You must use two peer Monitoring ports of the Sensor to deploy it full duplex mode. On the Sensor, the numbered ports are wired in pairs to accommodate the traffic.



 Note

- On NS7100, NS7200 and NS7300 Sensors, G0 and G3 indicate the fixed port slots. G1 and G2 indicate the slots for interface modules.
- In the following table, it is assumed that G1 is a 6-port RJ-45 1 Gbps/100 Mbps/10 Mbps interface module and G2 is the 8-Port SFP+/SFP 1/10G interface module. These interface modules can be interchanged.
- Since monitoring ports are internally wired, when you disable one of the ports in a pair, the corresponding port is also disabled.

The following Ethernet ports are coupled and must be used together.

Port Pairs	Sensor
G0/1 and G0/2	NS7300/NS7200/NS7100
G1/1 and G1/2	NS7300/NS7200/NS7100
G1/3 and G1/4	NS7300/NS7200/NS7100
G1/5 and G1/6	NS7300/NS7200/NS7100
G2/1 and G2/2	NS7300/NS7200/NS7100
G2/3 and G2/4	NS7300/NS7200/NS7100
G2/5 and G2/6	NS7300/NS7200/NS7100
G2/7 and G2/8	NS7300/NS7200/NS7100
G3/1 and G3/2	NS7300/NS7200/NS7100
G3/3 and G3/4	NS7300/NS7200/NS7100
G3/5 and G3/6	NS7300/NS7200/NS7100
G3/7 and G3/8	NS7300/NS7200/NS7100

:

## Cable types for routers switches hubs and computers

This section lists the types of cables that you require to connect the Sensor to other network devices:

- Use a crossover Ethernet RJ-45 cable to connect a router port to the SFP/SFP+ monitoring ports.
- Use a straight-through Ethernet RJ-45 cable to connect a switch or a hub port to SFP/SFP+ monitoring ports.
- Use a crossover Ethernet RJ-45 cable to connect a router port to computer to the Sensor Management port.
- Use a crossover Ethernet RJ-45 cable to connect a computer to the Sensor monitoring port.

:

## Connect the cables for in-line mode

In-line Gigabit Ethernet ports can be configured as fail-open or fail-closed. The RJ-45 monitoring ports are built-in and include an built-in fail-open functionality as well.

All other monitoring ports require the use of external active fail-open (AFO) kits for In-Line Fail-Open Active configuration.

Gigabit Ethernet ports fail-close, means the flow of traffic will stop if the Sensor fails. To allow traffic to flow uninterrupted, you must use special hardware, and cable the Sensor to external active fail-open kits. For instructions, see the subsequent sections of this chapter.

This section provides the steps to connect the Sensor's Gigabit Ethernet ports so they fail-close.

### Steps:

1. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports, for example G1/1.
2. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports, for example G1/2.



3. 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 and the one connected to 2 to the switch.

:

## Connect the cables for tap mode

To deploy the Sensor in tap mode, you must use a Sensor's Gigabit Ethernet Monitoring port pair with a third-party external tap.

 **Note**

For a list of Trellix-approved third party vendors, see the KnowledgeBase at <https://supportm.trellix.com>. Enter the relevant KnowledgeBase article in Search the Support Knowledge Center and click Search to locate the relevant KnowledgeBase article.

**Steps:**

1. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports, for example, G1/1.
2. Plug the cable appropriate for use with your transceiver module into one of the Monitoring ports labeled G1/2.
3. Connect the other end of each cable to the tap.
4. Connect the network devices that you want to monitor to the tap.

:

## Connect the cables for SPAN or hub mode

For the Sensor, monitoring in SPAN or hub mode occurs in in-line fail-open mode. When you monitor in SPAN or hub mode, you use only single ports.

To connect an Sensor to a SPAN port or hub, plug an LC fiber-optic or 45 cable into one of the modules and connect the other end of the cable to the SPAN port or the hub.

:

## Connect the cables for Sensor Fail-Open

The Fail-Open Kits minimize the potential risks of in-line Sensor failure on critical network links. You need to purchase these kits separately. Both copper and optical versions of the kit are available for the one-gigabit ports. The standard Gigabit Fail-Open Kits and 10 Gigabit Fail-Open Kits are available for the 1 and 10 gigabit ports respectively.

The Monitoring ports of the Sensors can be fail-close; thus, if the Sensor is deployed in-line fail-close, a hardware failure results in network downtime. Except the built-in RJ-45 ports which come with built-in fail-open functionality, you use the optional external bypass switch provided in an Active Fail-Open Kit for the Monitoring ports to fail-open.

While the Sensor is operating, the Active Fail-Open (AFO) kit is in-line and routes all traffic directly through the Sensor. When the Sensor fails, the switch automatically shifts to a bypass state; in-line traffic continues to flow through the network link but is no longer routed through the Sensor. After the Sensor resumes normal operation, the switch returns to the "inline" state, once again enabling in-line monitoring. The port pairs with AFO kits resume inline mode after a Sensor resumes normal operation or is in good health.

- G0 supports passive fail-open mode with RJ-11 port control

 **Note**

G0 also supports active fail-open using a Copper and Fiber 1/10 Gigabit AFO kit.

- G1 and G2 supports built-in fail-open and active fail-open mode for these interface modules:
  - 4-port 10 GigE/1 GigE LR Optical with internal fail-open
  - 4-port 10 GigE/1 GigE SR Optical 50 micron with internal fail-open
  - 4-port 10 GigE/1 GigE SR Optical 62.5 micron with internal fail-open
  - 4-port RJ-45 10 GigE with internal fail-open
  - 6-port RJ-45 1 GigE with internal fail-open

 **Note**

All RJ-45 ports support active fail-open using only a Copper AFO kit.

- 8-port SFP/SFP+ 1/10 Gigabit

 **Note**

The 8-port module supports active fail-open using a Copper and Fiber 1/10 Gigabit AFO kit.

- G3 supports both internal fail-open and active fail-open mode when connected to an Active Fail-Open (AFO) kit

 **Caution**

Sensor outage breaks the link connecting the devices on either side of the Sensor for a brief moment and requires the renegotiation of the network link between the two peer devices connected to the Sensor. Depending on the network equipment, this disruption introduced by the renegotiation of the link layer between the two peer devices might range from a couple of seconds to more than a minute with certain vendors' devices.

 **Caution**

A very brief link disruption might also occur while the links between the Sensor and each of the peer devices are renegotiated to place the Sensor back in in-line mode. This outage, again, varies depending on the device, and can range from a few seconds to more than a minute. The performance of the switchover from in-line to bypass and vice versa varies depending on the vendor.

You can find the installation and troubleshooting instructions for the kit in the guide that accompanies the kit. For example, for more information on the Optical kits, see the *1 Gigabit Optical Active Fail-Open Bypass Kit Guide* and *10 Gigabit Optical Active Fail-Open Bypass Kit Guide*.

:

## Connect the cable for Sensor failover

For Sensor failover, connect two NS7x00 Sensors using the standard LC-LC cables. These two Sensors must be running the same software version.

Purchase two 10G SFP+ and use the standard cables. Failover cables are additional hardware required to support failover communication between two NS7x00 Sensors.

### Note

Trellix does not ship the transceiver modules and cables with the NS7x00 Sensors. Please purchase the same separately for failover setup.

Refer to the following table before you configure a HA pair:

Sensor Model	Port to connect the HA pair	Cable requirements for failover
NS7300/NS7200/NS7100	G0/1	2 10G SFP+ and standard LC-LC cable

### Steps:

1. Plug the cable appropriate for use with your SFP+ module into port G0/1 of the active NS7x00 Sensor.
2. Connect the other end of the cable with SFP+ into port G0/1 of the standby NS7x00 Sensor.

:


## Turning the Sensor on and off

### Note

Do not attempt to turn on the Sensor until you have installed the Sensor in a rack and made all the necessary network connections.

### Steps:

1. Connect the power cable to the Sensor power inlet.
2. Connect the power cable to a power source.

 **Note**

If you are installing a redundant power supply, you should install it as described in *Install a new power supply* section. For true redundant operation with the optional redundant power supply, Trellix recommends that you plug each supply into a different power circuit.

The Sensor has no power switch. The Sensor turns on as soon as one of its power cables is connected to a power source. Trellix recommends that you use the **shutdown** CLI command to halt the Sensor before turning it off. For more information on CLI commands, see the *CLI commands* section in *Trellix Intrusion Prevention System Product Guide*

## Configure the Sensor and Manager for deployment

### 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.

#### Steps:


1. Prepare the system according to the requirements outlined in *Trellix Intrusion Prevention System Installation Guide*.
2. Close all open applications.
3. Go to [Trellix Download Server \(https://www.trellix.com/en-us/downloads/my-products.html\)](https://www.trellix.com/en-us/downloads/my-products.html).
4. Log on using your **Grant Number** and registered **Email Address**.  
The Find Products page opens.
5. In the Category filter, select Network Security.
6. Click on the Manager version required.  
The Available Downloads page opens.
7. In the Type filter, select Installation.  
The Manager installation files available for download are listed.
8. Click on the required Manager installation file and the download starts.

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

:

## Add the Sensor to the Manager

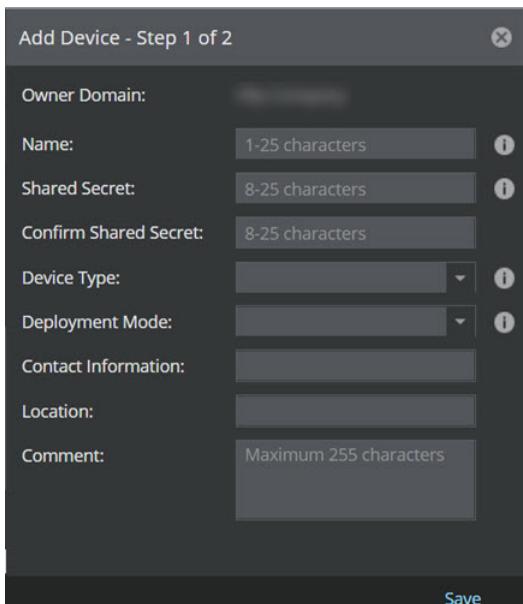
### Steps:

1. Log on to the Manager using the default user name (**admin**) and password (**admin123**).
2. Go to Devices → <Admin Domain Name> → Global → Device Manager.  
The Device Manager page is displayed.
3. 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.



4. Enter the following mandatory information in the appropriate fields:

- Name — The Sensor name must begin with a letter. The maximum length of the name is 25 characters.
- 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 enter later 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.

- Device Type — Specifies the type of device to be added. Select IPS Sensor.
- Deployment Mode — Select Direct or Indirect.

 **Note**

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

- Contact Information — (Optional) Type the contact information.
- Location — (Optional) Type the location.
- Comment — (Optional) Type the comment.

5. Click Save.

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

:

## 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.

**Steps:**

1. Log on to the Sensor using the terminal connected to the Console port.
2. At the prompt, log on using the default Sensor username (**admin**) and password (**admin123**).



```

login as: admin
* * *

Authorized users only. Unauthorized users will be prosecuted
to the full extent of the law.

* * *
Using keyboard-interactive authentication.
Password:
Last login: Fri Sep 28 07:20:31 2012 from 172.16.230.77
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is 'off'.

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

```

- (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.

- 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.

At the prompt, type: **set sensor name <word>**. 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.

- 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**
- 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**

7. 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.

8. If prompted, reboot the Sensor. Type **reboot**

 **Note**

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

9. 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 that the information is correct.
10. 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.

11. Type **show** to verify the configuration information. Check that all information is correct.
12. Type **exit** to exit the session.

:

## Verify successful installation

### Steps:

1. Type **status** in the Sensor CLI. The status report appears.

```

intruShell@ns > status
[Sensor]
System Initialized      : yes
System Health Status   : good
Layer 2 Status         : normal (IDS/IPS)
Installation Status    : complete
IPv6 Status            : Dont Parse and Allow Inline
Reboot Status          : Not Required
Guest Portal Status    : up
Hitless Reboot         : Available
Last Reboot reason     : reboot issued from NSM

[Signature Status]
Present                : yes
Version                : 1.0.0
Power up signature     : good
Geo Location database  : Present
DAT file               : Present
DAT file Version       : 1937.0

[Manager Communications]
Trust Established      : yes (RSA 2048-bit with SHA2 support)
Alert Channel         : up
Log Channel           : up
Authentication Channel : up
Last Error            : None
Alerts Sent           : 344630
Logs Sent             : 208586

[Alerts Detected]
Signature              : 8507809   Alerts Suppressed : 8322935
Scan                  : 3282     Denial of Service : 1113
Malware                : 0

[McAfee MACTD Communication]
Status                : down
IP                    : 0.0.0.0
Port(Secure)         : 8505

```

The Sensor parameter **System Initialized** should be **yes**, and for Manager communication **Trust Established** should be **yes**.

- Return to the Manager. In the Manager Home page, view the Manager status in the System Faults section. The Manager status should be up and Sensor status should be active.

System Faults					
Manager	Status	Critical	Error	Warning	
Manager	Up	1	1	0	
Device	Status	Critical	Error	Warning	
Doc_NS-series_Sensor_1	Active	6	0	3	
Doc_NS-series_Sensor_2	Active	4	1	3	
NS9500_Stack-1	Unknown	0	0	0	
NS9500_Stack-2	Unknown	0	0	0	
NSP_Doc_Sensor_1	Active	0	0	0	
NSP_Doc_Sensor_2	Active	1	0	0	
NSP_Doc_VM600_1	Active	0	0	0	
NSP_Doc_VM600_2	Active	0	0	0	

- From the Manager Home page, click Configure to open the Configuration page.
- Select your added Sensor: Device List → <Device\_Name>. The ports for this Sensor appear under the <Device\_Name> node.

#### Note

<Device\_Name> indicates the name of the Sensor you added.

Port	Link	Virtual Adapter	Operation Mode	Placement	Response Port
I/O Module: G0 (2-port QSFP+ module detected)					
0/1	---	---	---	---	---
0/2	---	---	---	---	---
I/O Module: G1 (empty)					
---	---	---	---	---	---
I/O Module: G2 (empty)					
---	---	---	---	---	---
I/O Module: G3 (8-port RJ-45 module detected)					
3/1	⊘ Disabled		In-line Fail Open (Paired with 3/2)	Inside Network	This Port
3/2	⊘ Disabled		In-line Fail Open (Paired with 3/1)	Outside Network	This Port
3/3	✔ Up		In-line Fail Open (Paired with 3/4)	Inside Network	This Port
3/4	✔ Up		In-line Fail Open (Paired with 3/3)	Outside Network	This Port
3/5	✔ Up		In-line Fail Open (Paired with 3/6)	Inside Network	This Port
3/6	✔ Up		In-line Fail Open (Paired with 3/5)	Outside Network	This Port
3/7	⊘ Disabled		In-line Fail Open (Paired with 3/8)	Inside Network	This Port
3/8	⊘ Disabled		In-line Fail Open (Paired with 3/7)	Outside Network	This Port

- 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 IPS-provided policies, you can clone the policy and then customize it as described in *Trellix Intrusion Prevention System Product Guide*.
- Click Device List → <Device\_Name> → Port Settings.
- 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*.

:

## You're up and running!

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

### Steps:

- For detailed usage instructions, see *Trellix Intrusion Prevention System Product Guide*, or click the ? buttons in the upper-right corner of each window in the Manager.
- Start the Analysis → <Admin Domain> → Attack Log to view alert statistics as attacks are detected. A summary of alerts is displayed in the Unacknowledged Alert Summary monitor of the Manager Dashboard page.
- Having problems? Check *Trellix Intrusion Prevention System Product Guide* for troubleshooting information.

4. 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://supportm.trellix.com>.

:

## Troubleshooting the Sensor

This section lists some common installation problems, the possible causes, and the corresponding solutions.

Problem	Possible Cause	Solution
LED is off.	The Sensor is turned off.	Restore Sensor power.
LED is off.	The Sensor port cable is disconnected.	Check the Sensor cable connections.
Sensor is operational but is not monitoring traffic.	Network device cables have been disconnected.	Check the cables and make sure they are properly connected to both the network devices and the bypass switch.
Sensor is operational but is not monitoring traffic.	The Sensor ports have not been enabled in the Manager.	The Sensor will not monitor traffic on the ports unless the ports are enabled in the Manager. Ports are disabled in case of Sensor failure; you must re-enable them for Sensor monitoring to resume.
Network or link problems	Improper cabling or port configuration	Make sure that the transmitting and receiving cables are properly connected to the bypass switch.
Runts or giants errors on switch and routers	Improper cabling or port configuration	Make sure that the transmitting and receiving cables are properly connected to the bypass switch.

Problem	Possible Cause	Solution
The system fault "Switch absent" appears in the Manager Status page.	The Active Fail-Open Kit is disconnected.	Check the Active Fail-Open Kit and make sure it is properly connected to the Sensor.

## Sensor technical specifications

The following table lists the specifications of an NS7x00 Sensor:

Sensor Specifics	NS7300	NS7200	NS7100
Dimensions	17.5" (W) x 1.69" (H) x 28.9" (D)	17.5" (W) x 1.69" (H) x 28.9" (D)	17.5" (W) x 1.69" (H) x 28.9" (D)
Weight	31 lbs	31 lbs	29 lbs
Storage	Solid State 160 GB	Solid State 160 GB	Solid State 160 GB
<b>System Heat Dissipation</b>			
Maximum BTU	1298 BTU/hr	1298 BTU/hr	927 BTU/hr
Typical BTU	1113 BTU/hr	1113 BTU/hr	816 BTU/hr
Maximum Power Consumption	350 W	350 W	250 W
Redundant Power Supply	Optional	Optional	Optional
Power	100-240 VAC (50/60Hz)		

---

Sensor Specifics	NS7300	NS7200	NS7100
Temperature	Operating: 0°-35° C , Non-operating: - 40°-70° C		
Relative humidity (non-condensing)	Operational: 10% -90%, Non-operational: 5% -95%		
Altitude	0 to 10,000 feet		
Safety Certification	UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB license and report covering all national country deviations.		
EMI Certification	FCC Part 15, Class A (CFR 47) (USA) ICES-003 Class A (Canada), EN55022 Class A (Europe), CISPR22 Class A (Int'l)		

:

## NS5x00 Sensors

:

### About Sensors

Sensors are high-performance, scalable, and flexible content processing appliances built for accurate detection and prevention of:

- Network intrusions
- Network misuse
- Distributed Denial-of-Service (DDoS) attacks

Sensors are specifically designed to handle traffic at wire speed, efficiently inspect and detect intrusions with a high degree of accuracy, and are flexible enough to adapt to the security needs of any enterprise environment. When deployed at key network access points, the Sensor provides real-time traffic monitoring to detect malicious activity and respond to such activity based on the responses configured by the administrator.

After you deploy a Sensor successfully, you configure and manage it using the Manager. The process of configuring a Sensor and establishing communication with the Manager is described in the subsequent chapters of this guide. For details about the Manager, see the *Manager Administration* section in *Trellix Intrusion Prevention System Product Guide*.

:

### Functions of NS-series Sensors

The NS-series Sensors are a third-generation hardware platform Sensors designed for high bandwidth links to offer Next Generation IPS (NGIPS) capability and provide high aggregate throughput across various Sensor models. The following models are supported.

- NS5200 - The NS5200 Sensor is a 1RU unit providing an aggregate throughput of 1 Gbps
- NS5100 - The NS5100 Sensor is a 1RU unit providing an aggregate throughput of 600 Mbps

The primary function of a Sensor is to analyze traffic on selected network segments and to respond when an attack is detected. The Sensor examines the header and data portions of every network packet, looking for patterns and behavior in the network traffic that indicate malicious activity. The Sensor examines packets according to user-configured policies, or rule sets, which determine what attacks to watch for, and how to respond with countermeasures if such an attack is detected.

If an attack is detected, a Sensor responds according to its configured policy. The Sensor can perform many types of attack responses, including generating alerts and packet logs, resetting TCP connections, "scrubbing" malicious packets, and even blocking attack packets entirely before they reach the intended target.

:

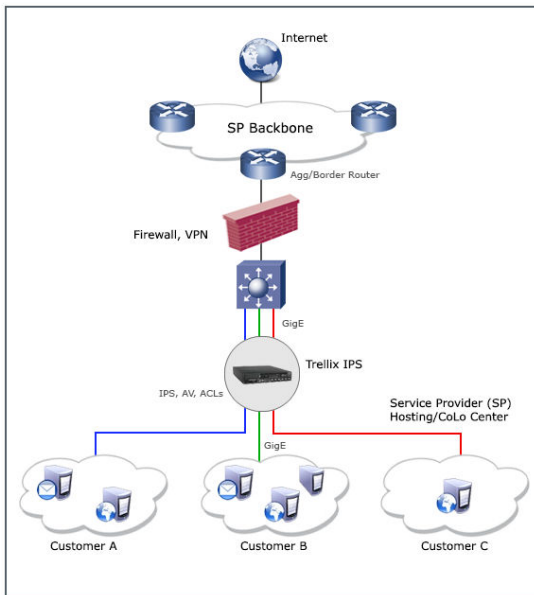


## Deployment of NS-series Sensors

Deployment of a Sensor requires knowledge of your network to help determine the level of configuration and the number of installed Sensors. You also need to determine the number of Trellix ePolicy Orchestrator - On-prem servers required to protect your network. The Sensor is purpose-built to monitor traffic across one or more network segments.

Following is an example of a network topology using Gigabit Ethernet throughput. In the illustration, Trellix Intrusion Prevention System provides IPS protection to outsourced servers. High port-density and virtualization provides a highly scalable solution, while Trellix IPS protects against web and eCommerce mail server exploits.

### A sample NS-Series Sensor deployment



:

## NS5x00 Sensor physical description

The high-port density NS-series Sensor is designed for high bandwidth links. This section gives a physical description of the NS5x00 Sensors.

The NS5200 and NS5100 Sensor models that provide 1 Gbps and 600 Mbps throughput respectively.

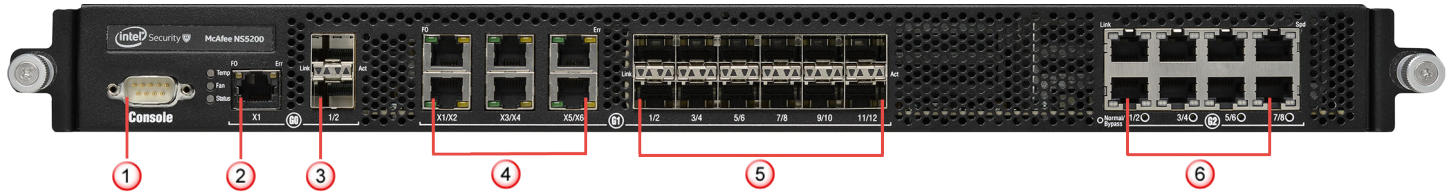
:

### Components of an NS5x00 Sensor

The NS5x00 front and rear panel details are described below.

## The NS5100/NS5200 Sensor model

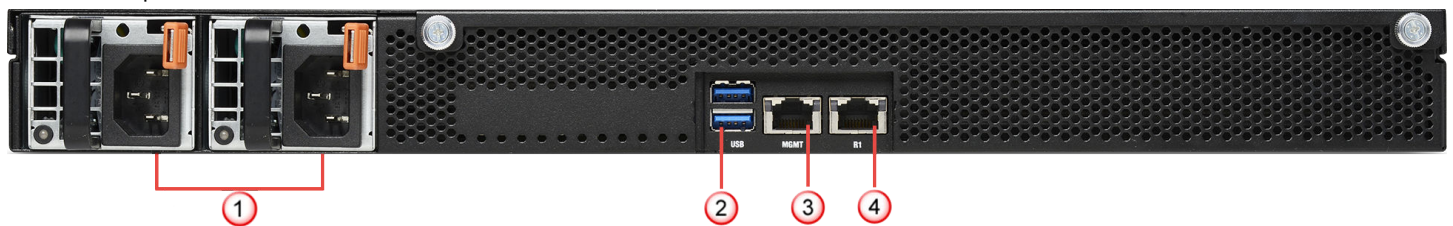
### Sensor front panel



1. Console port (1)
2. RJ-11 port (1) for fail-open control of two built-in SFP+ ports in slot G0. The RJ-11 ports support 1 Gbps (SFP) fiber and 10 Gbps (SFP+) (SR and LR). You can convert these ports to copper ports by using the copper SFP transceivers.
3. SFP/SFP+ 1/10 fiber Gigabit or SFP 1 Gbps copper Ethernet ports (2)
4. RJ-11 port (6) for external passive fail-open control of twelve SFP ports in slot G1. The RJ-11 ports support 1 Gbps (SFP) fiber (SR and LR). You can convert these ports to copper ports by using the copper SFP transceivers. The fail-open ports are internally wired to control the SFP ports. For example, port X1 controls monitoring ports G1/1 and G1/2; port X2 controls monitoring ports G1/3 and G1/4 and so on.
5. SFP 1 Gbps copper or fiber Gigabit Ethernet ports (12)
6. RJ-45 10/100/1000 Mbps Ethernet Monitoring ports (8)

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

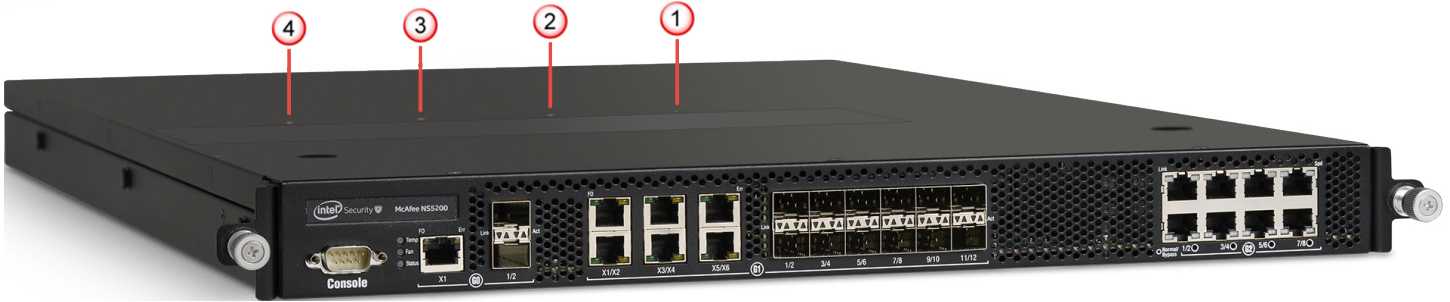
### Sensor rear panel



1. Power supply inlet (2)
2. USB ports (2)
3. RJ-45 10/100/1000 Management port (MGMT) (1)
4. RJ-45 10/100/1000 Response port (R1) (1)

The NS5x00 Sensors have four fan units on the top.

### Fan units-NS5100/NS5200



The direction of airflow in all the Sensors is front to back. Cold air enters through the front of the chassis.

### Note

The fan units and power supplies are field replaceable.

The following table gives the details of the supported ports.

Ports	NS5100/NS5200
Fixed RJ-45 ports (internal fail-open)	8
Fixed SFP 1 Gbps ports	12
Fixed 10 GigE/1 GigE (SFP+/SFP) ports	2
Fixed RJ-11 ports (external passive fail-open)	6
Dedicated Response ports (RJ-45)	1 (1G/100M/10M)
Dedicated Management ports (RJ-45)	1 (1G/100M/10M)
Dedicated Auxiliary port (DB9)	1
USB ports	2

- **Console port** — Use to set up and configure the Sensor using the CLI.
- **RJ-11 port** — Controls the SFP/SFP+ 1/10 Gigabit Ethernet port pair in passive fail-open mode
- **SFP/SFP+ 1/10 gigabit ethernet ports** — Enables you to monitor two SPAN ports or one in-line segment

- **RJ-45 10/100/1000 Mbps ethernet monitoring ports** — Enables you to monitor eight SPAN ports, four segments in-line, or a combination
- **External USB ports** — Use these in troubleshooting situations for system recovery purposes. You need to restart the Sensor through the USB storage device.
- **RJ-45 10/100/1000 Management port** — Use for communication with the Manager server. You can assign an IP address to this port during installation.
- **RJ-45 10/100/1000 Response port** — When you operate this port in SPAN or tap mode, it enables you to inject response packets back through a switch or a router.
- **Power Supply** — Power supply is included with an NS5x00 Sensor. The supply uses a standard IEC port (IEC320-C13). Trellix provides a standard, 2 m NEMA 5-15P (US) power cable (3 wire). International customers must procure a country-appropriate power cable.

The NS-series Sensor does not have internal taps; you must use it with a third-party external tap to run it in tapped mode.

:

## Sensor LEDs

The front and rear panel LEDs provide status information for the health of the Sensor and the activity on its ports. The following table describes the NS-series LEDs.

### Front panel LEDs

LED	Status	Description
Status	Green Amber	Sensor is operating in good health. Sensor is booting up. It also indicates system bad health.
Fan	Green Amber	All the fans are operating. One or more fans are not working.
Temp	Green Amber	Inlet air temperature measured inside the chassis is normal. (Chassis temperature OK) Inlet air temperature measured inside the chassis is too high. (Chassis temperature too hot)

LED	Status	Description
Gigabit Ports Act	Blinking Amber Off	Data is received or transmitted. No data is being transferred.
Gigabit Ports Link	Green Off	The link is up. The link is down.
Normal/Bypass	Green Off	The port pair is in Inline Fail-Open/Inline Fail-Close/SPAN/Tap Mode. The Port Pair is in the Bypass Mode.
Gigabit Ports Speed	Green Amber Off	Port speed is 1 Gbps. Port speed is 100 M. Port speed is 10 M.

### Rear panel LEDs

LED	Status	Description
Power	Solid Green Blinking Green Solid Amber	Power supply has power feed and is functioning. Power Supply is stand-by. It also indicates load sharing. Power Supply is not functioning or the unit has no power feed.
Management Port Speed	Green Amber Off	The port speed is 1000 Mbps. The port speed is 100 Mbps. The port speed is 10 Mbps.
Management Port Link	Green Off	The link is up. The link is down.
Response Port Speed	Green	The port speed is 1000 Mbps.

LED	Status	Description
	Amber Off	The port speed is 100 Mbps. The port speed is 10 Mbps.
Response Port Link	Green Off	The link is up. The link is down.

:

## Before you install

This chapter describes best practices for deployment of Sensors in your network. Topics include safety considerations for handling the Sensor, usage restrictions that apply to the Sensor model, and contents that are shipped along with the Sensor.

:

### Usage restrictions

The following restrictions apply to the use and operation of a Sensor:

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

:

### Safety measures

Please read the following warnings before you install the Sensor. These safety measures apply to all Sensor models unless otherwise noted. Failure to observe these safety warnings could result in serious physical injury.

#### Warnings:

- Read the installation instructions before you connect the system to its power source.
- To remove all power from the Sensor, unplug all power cords, including the redundant power cord.
- Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
- Before working on the equipment that is connected to power lines, remove all jewelry including rings, necklaces, and watches. Metal objects will heat up when connected to power and ground, and can cause serious burns or weld the metal object to the terminals.

- This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.
- Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Blank faceplates and cover panels prevent exposure to hazardous voltages and currents inside the chassis. The chassis contains electromagnetic interference (EMI) that might disrupt other equipment and direct the flow of cooling air.
- To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Exercise caution when connecting cables.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the users will be required to correct the interference at their own expense.
- Refer to the Appendix for information on regulatory, compliance, and other safety requirements.

:

### About fiber-optic ports

The Sensor uses fiber-optic connectors for its monitoring ports. The connector type is an SFP/SFP+ fiber-optic connector that is LC-duplex compatible.

Note the following:

- Fiber-optic ports (for example, SFP/SFP+, FDDI, OC-3, OC-12, OC-48, ATM, GBIC, and 100BaseFX) are considered Class 1 laser or Class 1 LED ports.
- These products have been tested and found to comply with Class 1 limits of IEC 60825-1, IEC 60825-2, EN 60825-1, EN 60825-2, and 21CFR1040.

#### Caution

To avoid exposure to radiation, do not stare into the aperture of a fiber-optic port. Invisible radiation could be emitted from the aperture of the port when no fiber cable is connected.

- Only FDA registered, EN 60825-1 and IEC 60825-1 certified Class 1 SFP/SFP+/ laser transceivers are acceptable for use with the Sensor.

:

### Contents of 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

:

## Unpack the Sensor

### Steps:

1. Open the crate.
2. Remove the first accessory box.
3. Verify you have received all parts. These parts are listed on the packing list and in the *Contents of the box* section.
4. Place the Sensor box as close to the installation site as possible.
5. Position the box with the text upright.
6. Open the top flaps of the box.
7. Remove the accessory box within the Sensor box.
8. Verify you have received all parts. These parts are listed on the packing list and in the *Contents of the box* section.
9. Remove the Slide Rail Kit.
10. Pull out the packing material surrounding the Sensor.
11. Remove the Sensor from the antistatic bag.
12. Save the box and packing materials for later use in case you need to move or ship the Sensor.

:

## Setting up the Sensor

This chapter describes how to set up the Sensor for you to configure it.

:

### Setup overview

Setting up a Sensor involves these steps:

1. Position the Sensor as described in the section [How to position the Sensor](#).
2. Attach power, network, and monitoring cables.
3. Turn on the Sensor.
4. Configure the Sensor after you have set up and turned it on.

:

### How to position the Sensor



Place the Sensor in a physically secure location, close to the switches or routers it will be monitoring. Ideally, the Sensor must be located within a standard communications rack. To mount the Sensor on a rack, you will attach two mounting rails to the Sensor as described in the subsequent sections of this guide.

:

## Install the slide rails and rack-mount the Sensor

Trellix recommends rack-mounting your Sensor. For maintenance purposes, you must have access to the front and rear of the Sensor.

### Caution

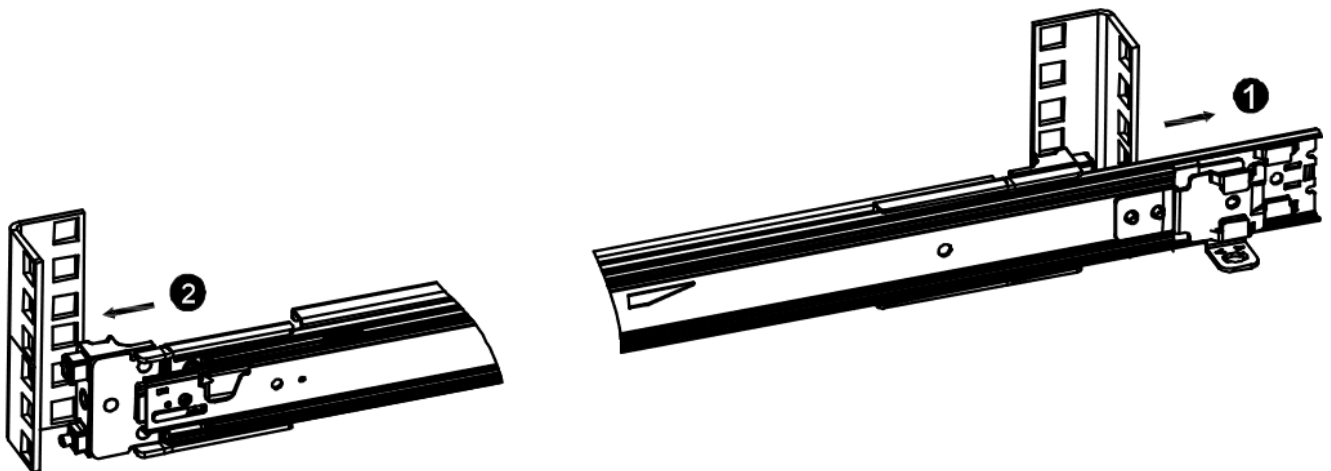
Before you mount the Sensor on the rack, make sure that the power is off. Remove the power cable and all network interface cables from the Sensor.

### Important

Due to the weight of the appliance, Trellix recommends that one person holds the chassis and the other person fixes it to the rail cabinet.

#### Steps:

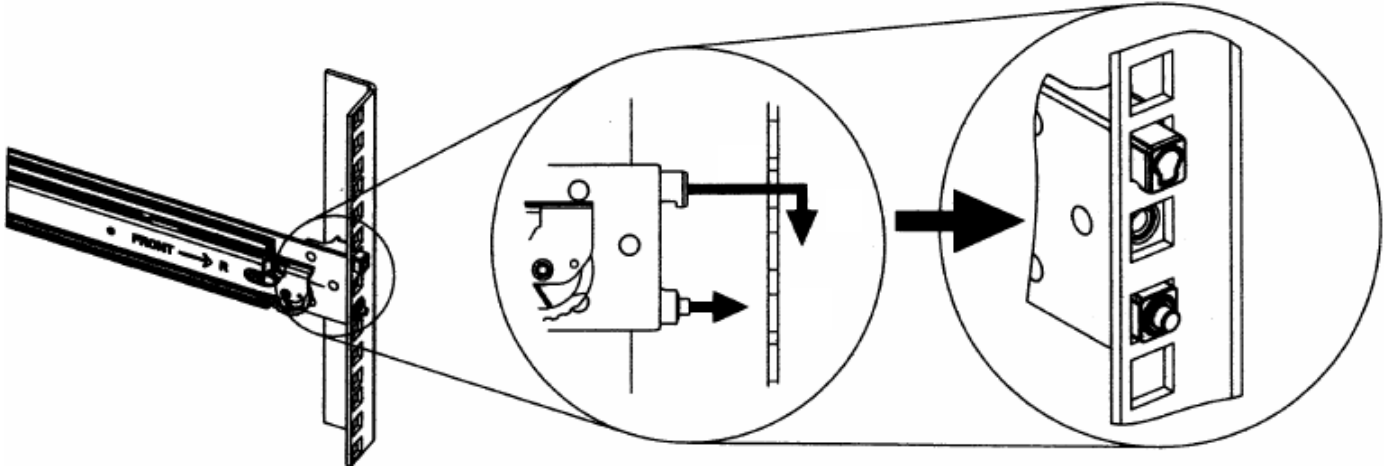
1. Mount the slide rails to the rack.
  - a. Align the rails and fit it into the corresponding holes on the front post of the rack.
  - b. Fit the rails into holes on the rear post of the rack.



- c. Install the front end of each slide rail in the front post of a 4-post enterprise rack. Try different hole combinations until one of them locks in.

 Tip

At times in a 4-post enterprise rack, certain hole combinations do not permit the rail latch to lock in. So to make it lock, you must try different hole combinations.

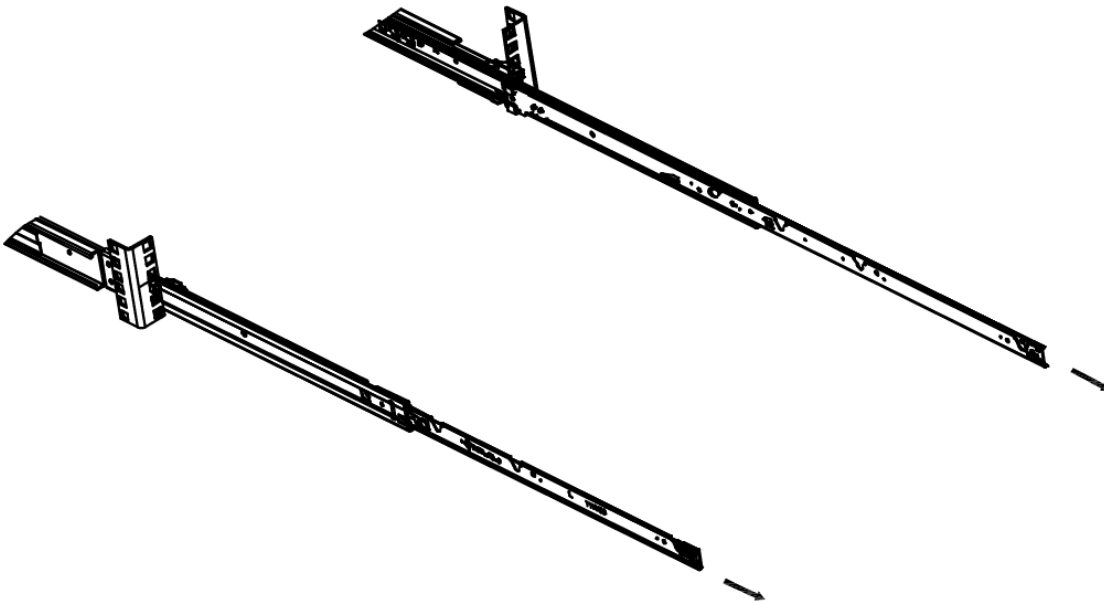


2. Position the inner members to fix the chassis.
  - a. Pull inner member of the slide rail out until it comes to a lock position.

 Tip

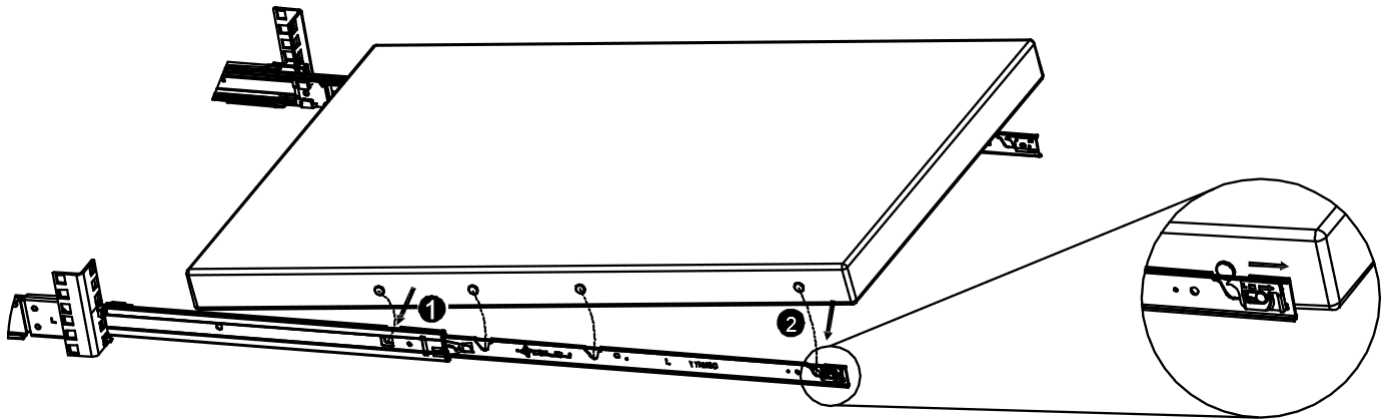
To push the inner member into the rack, lift the latch, and push the inner member.

- b. Position both inner members.

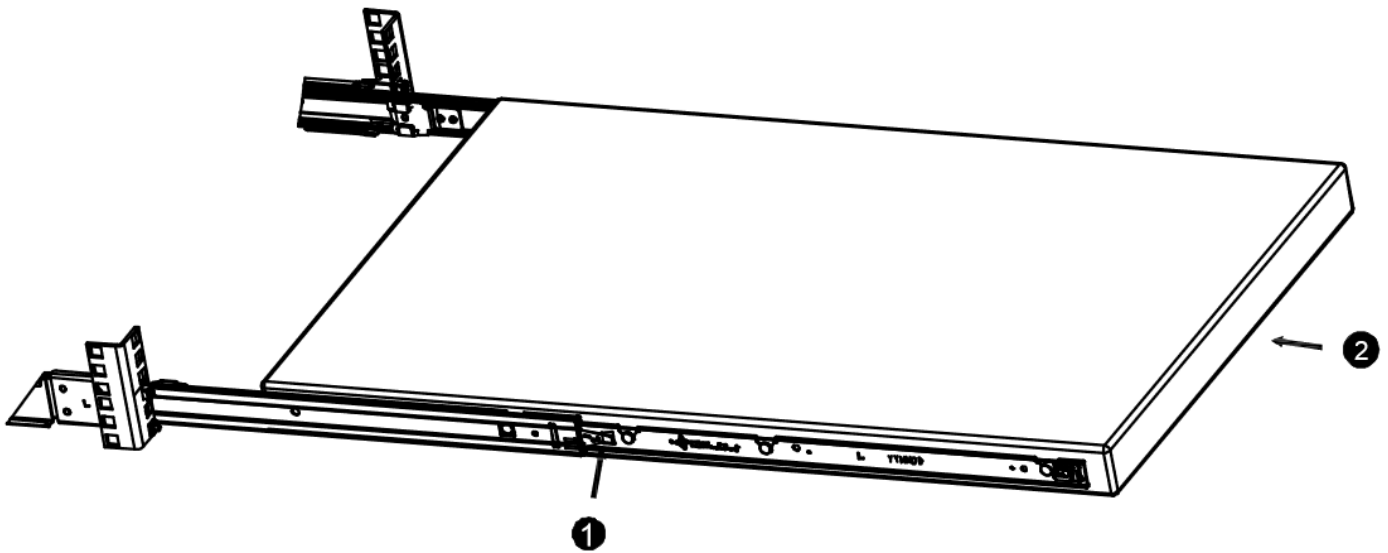


3. Mount inner members to the chassis unit.

- a. Place each inner member on both sides of the chassis unit. Position the mounting holes of the inner member with matching mounting hooks on chassis unit.
- b. Apply to both sides of chassis unit.



4. Install chassis unit into the rack.
  - a. Lift the release tab on both sides and push the inner members into the outer members until they lock in place.
  - b. Continue to push the chassis unit in until fully closed.



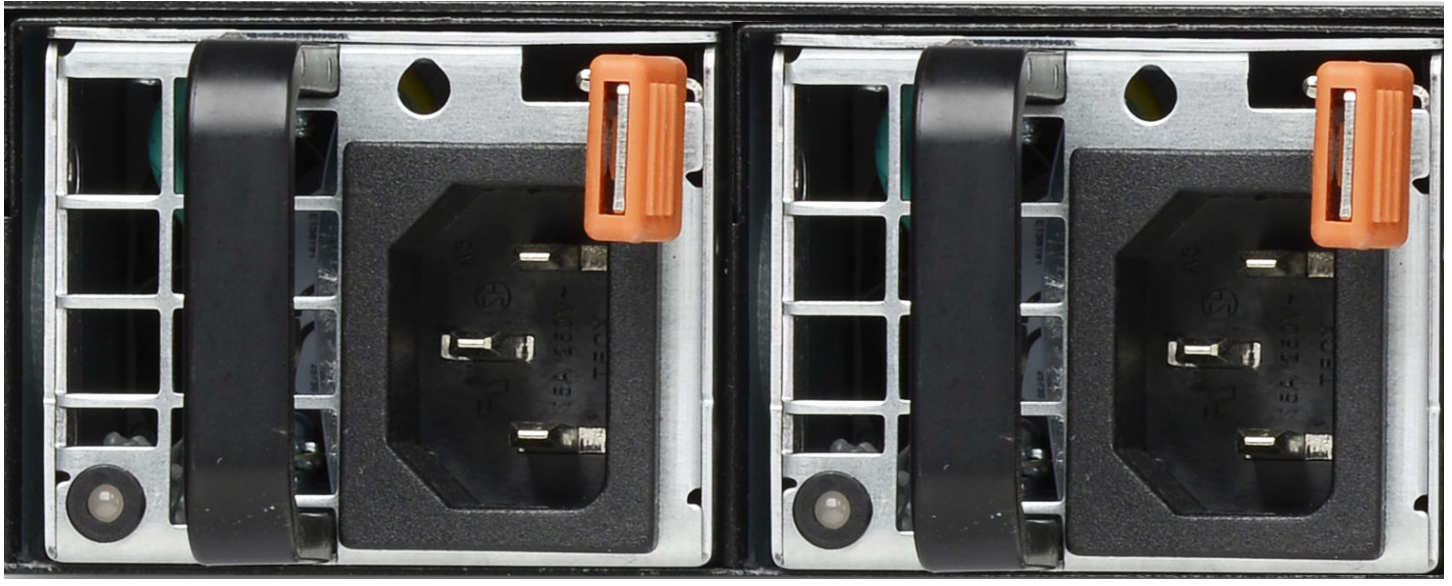
5. Secure the chassis unit through the rack rails.
  - a. With the chassis unit in fully closed position, secure using two spring screws provided in the chassis ear.
  - b. Tighten the screws. The screws thread directly to the rack posts.

:

## Redundant power supply

The basic configuration of a Sensor includes two hot-swappable power supplies. Each of these modules has one handle for insertion or extraction from the unit as well as a release latch. If you have purchased an additional power supply from Trellix, refer to the following sections to remove and install the new power supply.

Power supply units



:

## Install a new power supply

Steps:

1. Unpack the power supply from its shipping carton.
2. Remove the faceplate panel covering the power supply slot.

 **Note**

The faceplate panel must remain in place unless a power supply is in the power supply slot. Do not operate the Sensor without the faceplate panel in place.

3. Place the power supply in the slot with the cable outlet facing front and on the left side of the faceplate.
4. Slide in the power supply until it makes contact with the backplane, then push firmly to mate the connectors solidly with the backplane.

 **Note**

For true redundant operation with the power supply, Trellix recommends that you plug each supply into a different power circuit. For optimal protection, use uninterruptible power sources.

:

## Remove the power supply

Perform this task if you want to remove the power supply from the Sensor.

### Steps:

1. Unplug the power cable from its power source and remove the power cable from the power supply.
2. Push the release latch sideways toward the handle.
3. Center the handle of the power supply and pull on it to remove the power supply.
4. Use faceplate panels to protect unused slots from dust and to reduce electromagnetic radiation.
5. Replace the mounting bracket.

### Caution

To avoid data interruption, do not turn off both power supplies on an in-line Sensor; or else the Sensor shuts down and all Sensor functions stop. Turn off only the power supply that you are replacing.

### Note

To remove all power from the Sensor, unplug all power cords.

## Small form-factor pluggable transceiver modules

The NS5x00 Sensors use two types of small form-factor pluggable transceiver modules as shown in the following table. For more information, see the *NS-series Transceiver Modules* section in *Trellix Intrusion Prevention System NS-series Reference Guide*.

Type	Performance
SFP	1 Gbps (fiber-optic) 1 Gbps (copper)
SFP+	< 10 Gbps (fiber-optic)

Each module is an input/output device that plugs into an LC-type Gigabit Ethernet port, linking the port with a copper or fiber-optic network. SFP optical interfaces are less than half the size of GBIC interfaces.

To ensure compatibility, Trellix supports only those SFP, SFP+, QSFP+ and QSFP28 modules purchased through Trellix or from a Trellix-approved vendor. For a list of approved vendors, locate the relevant KnowledgeBase article at <https://>

[supportm.trellix.com](http://supportm.trellix.com). Enter the relevant KnowledgeBase article in Search the Support Knowledge Center and click Search to locate the article.

These installation instructions provide information for installing SFP and SFP+ modules that use a bail clasp for securing the module in place in the Sensor. Your module might be slightly different. Check the module manufacturer's installation instructions for more details. For ease of installation, insert the module in the Sensor when it is turned off and before placing it on a rack.

### Caution

To prevent eye damage, do not stare into open laser apertures.

:

## Install a transceiver module

### Steps:

1. Remove the module from its protective packaging.
2. Locate the label on the module and make sure that the alignment groove is down.
3. Grip the sides of the module with your thumb and forefinger and insert the module into the module socket. Modules are keyed to prevent incorrect insertion.

---

Insert a transceiver module



:

## Remove a transceiver module

Perform these tasks if you need to remove a module.

### Steps:

1. Disconnect the network fiber-optic cable from the module.
2. Release the module from the slot by pulling the bail clasp out of its locked position.
3. Slide the module out of the slot.
4. Insert the module plug into the module optical bore for protection.

:

## Attaching cables to the Sensor

Follow the steps outlined in this chapter to connect the cables to the various ports of your Sensor.

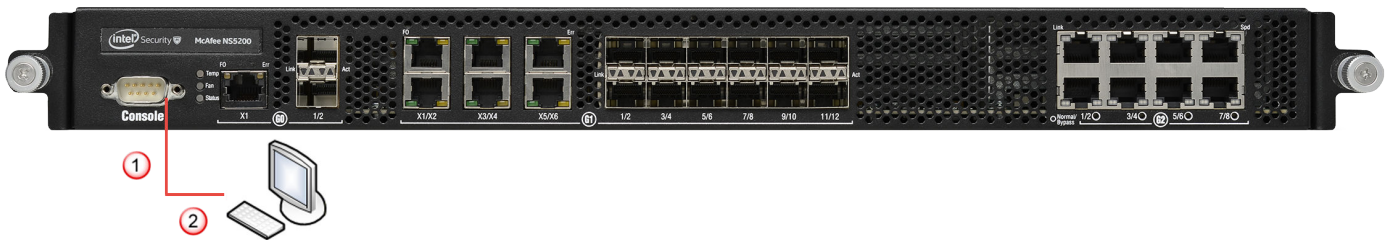
:

### Connect the cable to the Console port

The Console port on the NS5x00 Sensor is used for setup and configuration of the Sensor.

### Steps:

1. For console connections, plug in the DB9 Console cable supplied by Trellix into the Console port on the Sensor. This port is labeled **Console** in the Sensor front panel.



2. Connect the other end of the Console port cable directly to a COM port of the computer or terminal server you will use to configure the Sensor, for example, a computer 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. Required settings for HyperTerminal are listed below:

Name	Setting
Baud rate	115200
Number of bits	8

Name	Setting
Parity	None
Stop bits	1
Flow control	None

3. Turn on the Sensor.

:

### Connect the cable to the Response port

While operating in tap or SPAN mode, the Sensor uses its Response port to respond to attacks. When deployed in tap mode, the Sensor does not inject response packets through the tap but uses the Response port.

#### Steps:

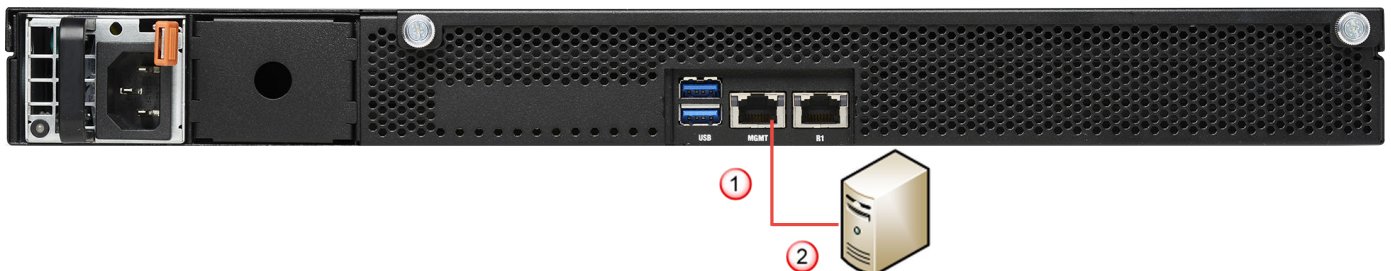
1. Plug a Cat-5e Ethernet cable into the Response port. This port is labeled **R1** on the Sensor rear panel.
2. Connect the other end of the cable to the network device, such as a hub, switch, or a router, through which you want the Sensor to respond to attacks.

:

### Connect the cable to the Management port

The Sensor communicates with the Manager using the Management port.

1. Plug a Category 5e Ethernet cable into the Management port. This port is labeled **MGMT** in the rear panel of the NS5x00 Sensor.



2. Plug the other end of the cable into the network device connected to your Manager server.



 **Note**

To isolate and protect your management traffic, Trellix strongly recommends you to use a separate, dedicated management subnet to interconnect the Sensors and the Manager.

:

## About connecting cables to the Monitoring ports

Connect to network devices that will send traffic to the Sensor monitoring ports. You can deploy Sensors in the following operating modes:

- Inline Fail Open
- Inline Fail Open – Active
- Inline Fail Open – Passive
- Inline Fail Closed
- SPAN or Hub
- Tap

:

## How to use peer ports

You must use two peer monitoring ports of the Sensor to deploy it full-duplex mode. On the Sensor, the numbered ports are internally wired in pairs to accommodate the traffic.

 **Note**

- On NS5100 and NS5200 Sensors, G0, G1, and G2 indicate fixed port slots.
- Since monitoring ports are internally wired, when you disable one of the ports in a pair, the corresponding port is also disabled.

The following ethernet ports are coupled and must be used together.

Port Pairs	Sensor
G0/1 and G0/2	NS5200/NS5100
G1/1 and G1/2	NS5200/NS5100
G1/3 and G1/4	NS5200/NS5100

Port Pairs	Sensor
G1/5 and G1/6	NS5200/NS5100
G1/7 and G1/8	NS5200/NS5100
G1/9 and G1/10	NS5200/NS5100
G1/11 and G1/12	NS5200/NS5100
G2/1 and G2/2	NS5200/NS5100
G2/3 and G2/4	NS5200/NS5100
G2/5 and G2/6	NS5200/NS5100
G2/7 and G2/8	NS5200/NS5100

:

## Cable types for routers, switches, hubs, and computers

This section lists the types of cables that you require to connect the Sensor to other network devices:

- Use a crossover Ethernet RJ-45 cable to connect a router port to the SFP/SFP+ monitoring ports.
- Use a straight-through Ethernet RJ-45 cable to connect a switch or a hub port to SFP/SFP+ monitoring ports.
- Use a crossover Ethernet RJ-45 cable to connect a router port to computer to the Sensor Management port.
- Use a crossover Ethernet RJ-45 cable to connect a computer to the Sensor monitoring port.

:

## Connect the cables for in-line mode

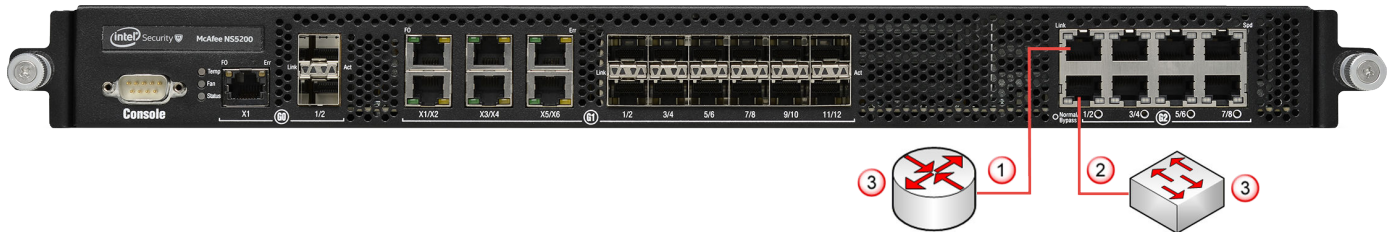
In-line gigabit ethernet ports can be configured as fail-open or fail-closed. The RJ-45 monitoring ports are built-in and include an built-in fail-open functionality as well.

All other monitoring ports require the use of external active or passive fail-open kits for Inline Fail Open - Active and Inline Fail Open - Passive configurations.

Gigabit Ethernet ports fail close, implying that the flow of traffic will stop if the Sensor fails. To allow traffic to flow uninterrupted, you must use special hardware, and cable the Sensor to external active fail-open kits. For instructions, see the subsequent sections of this chapter.

This section provides steps to connect the Sensor's gigabit ethernet ports so they fail-close.

1. Plug the cable appropriate for use, with your transceiver module, into one of the monitoring ports, for example G2/1.
2. Plug the cable appropriate for use, with your transceiver module, into the other monitoring port, for example G2/2.



3. 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 and the one connected to 2 to the switch.

:

## Connect the cables for tap mode

To deploy the Sensor in tap mode, you must use a Sensor's gigabit ethernet monitoring port pair with a third-party external tap.

### Note

For a list of Trellix-approved third party vendors, see the KnowledgeBase at <https://supportm.trellix.com>. Enter the relevant KnowledgeBase article in Search the Support Knowledge Center and click Search to locate the relevant KnowledgeBase article.

#### Steps:

1. Plug the cable appropriate for use with your transceiver module into one of the monitoring ports, for example, G1/1.
2. Plug the cable appropriate for use with your transceiver module into one of the monitoring ports labeled G1/2.
3. Connect the other end of each cable to the tap.
4. Connect the network devices that you want to monitor to the tap.

:

## Connect the cables for SPAN or hub mode

For the Sensor, monitoring in SPAN or hub mode occurs in in-line fail-open mode. When you monitor in SPAN or hub mode, you use only single ports.

To connect an Sensor to a SPAN port or hub, plug an LC fiber-optic or RJ-45 cable into one of the port and connect the other end of the cable to the SPAN port or the hub.

:

## Connect the cables for Sensor Fail-Open

Fail-Open kits minimize the potential risks of in-line Sensor failure on critical network links. You need to purchase these kits separately. Both copper and optical versions of the kit are available for the one-gigabit ports.

Monitoring ports of the Sensors can be fail-close; thus, if the Sensor is deployed in-line fail-close, a hardware failure results in network downtime. Except the built-in RJ-45 ports (G2) which come with built-in fail-open functionality, you use the optional external bypass switch provided in an active or passive fail-open kits for the other monitoring ports (G0, G1) to fail-open.

While the Sensor is operating, the active or passive fail-open kits is in-line and routes all traffic directly through the Sensor. When the Sensor fails, the fail-open switch automatically shifts to a bypass state; in-line traffic continues to flow through the network link but is no longer routed through the Sensor. After the Sensor resumes normal operation, the switch returns to the in-line state, enabling in-line monitoring.

- G0 supports active and passive fail-open modes using a copper and fiber 1 Gigabit kit with RJ-11 control port and SFP+(10G) Fiber fail-open kit.
- G1 supports both active and passive fail-open modes. G1 supports 1G SFP fiber and copper active/passive fail-open kits.
- G2 supports internal fail-open and supports active fail-open when connected to an active fail-open kit.

### Caution

Sensor outage breaks the link connecting the devices on either side of the Sensor for a brief moment and requires renegotiation of the network link between the two peer devices connected to the Sensor. Depending on the network equipment, this disruption introduced by the renegotiation of the link layer between the two peer devices might range from a couple of seconds to more than a minute with certain vendors' devices.

### Caution

A very brief link disruption might also occur when links between the Sensor and each of the peer devices are renegotiated to place the Sensor back in in-line mode. This outage, again, varies depending on the device, and can range from a few seconds to more than a minute. The performance of the switchover from in-line to bypass and vice versa varies depending on the vendor.

You can find the installation and troubleshooting instructions for the kit in the guide that accompanies the kit. For example, for more information on the Optical kits, see the *1 Gigabit Optical Active Fail-Open Bypass Kit Guide*.

:

## Connect the cable for Sensor failover

For Sensor failover, connect two NS5x00 Sensors using the appropriate cables. These two Sensors must be running the same software version.

Purchase four 1G SFPs and use the appropriate fiber or copper cable. Failover cables are additional hardware required to support failover communication between two NS5x00 Sensors.

### Note

Trellix does not ship the transceiver modules and cables with the NS5x00 Sensors. Please purchase the same separately for failover setup.

Refer to the following table before you configure a HA pair:

Sensor Model	Port to connect the HA pair	Cable requirements for failover
NS5100/NS5200	G1/1, G1/2	4 1G SFP and appropriate fiber or copper cable

### Steps:

1. Plug the cables appropriate for use with your SFP modules into both ports, G1/1 and G1/2 of the active NS5x00 Sensor.
2. Connect the other end of the respective cables with SFP modules into both ports, G1/1 and G1/2 of the standby NS5x00 Sensor. Both G1/1 and G1/2 connections are needed for failover to work properly.

:

## Turning the Sensor on and off

### Note

Do not attempt to turn on the Sensor until you have installed the Sensor in a rack and made all the necessary network connections.

### Steps:

1. Connect the power cable to the Sensor power inlet.
2. Connect the power cable to a power source.

 **Note**

If you are installing a redundant power supply, you should install it as described in *Install a new power supply* section. For true redundant operation with the power supply, Trellix recommends that you plug each supply into a different power circuit.

The Sensor has no power switch. The Sensor turns on as soon as one of its power cables is connected to a power source. Trellix recommends that you use the **shutdown** CLI command to halt the Sensor before turning it off. For more information on CLI commands, see the *CLI commands* section in *Trellix Intrusion Prevention System CLI Guide*.

## Configure the Sensor and Manager for deployment

### 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.

#### Steps:


1. Prepare the system according to the requirements outlined in *Trellix Intrusion Prevention System Installation Guide*.
2. Close all open applications.
3. Go to [Trellix Download Server \(https://www.trellix.com/en-us/downloads/my-products.html\)](https://www.trellix.com/en-us/downloads/my-products.html).
4. Log on using your **Grant Number** and registered **Email Address**.  
The Find Products page opens.
5. In the Category filter, select Network Security.
6. Click on the Manager version required.  
The Available Downloads page opens.
7. In the Type filter, select Installation.  
The Manager installation files available for download are listed.
8. Click on the required Manager installation file and the download starts.

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

:

## Add the Sensor to the Manager

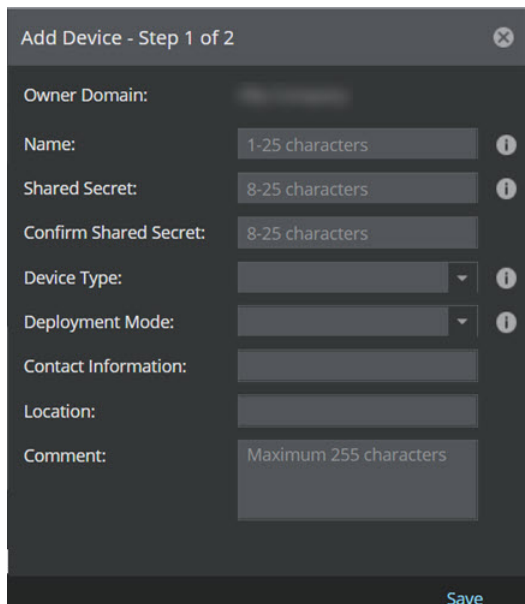
### Steps:

1. Log on to the Manager using the default user name (**admin**) and password (**admin123**).
2. Go to Devices → <Admin Domain Name> → Global → Device Manager.  
The Device Manager page is displayed.
3. 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.



4. Enter the following mandatory information in the appropriate fields:

- Name — The Sensor name must begin with a letter. The maximum length of the name is 25 characters.
- 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 enter later 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.

- Device Type — Specifies the type of device to be added. Select IPS Sensor.
- Deployment Mode — Select Direct or Indirect.

 **Note**

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

- Contact Information — (Optional) Type the contact information.
- Location — (Optional) Type the location.
- Comment — (Optional) Type the comment.

5. Click Save.

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

:

## 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.

**Steps:**

1. Log on to the Sensor using the terminal connected to the Console port.
2. At the prompt, log on using the default Sensor username (**admin**) and password (**admin123**).



```

login as: admin
* * *

Authorized users only. Unauthorized users will be prosecuted
to the full extent of the law.

* * *
Using keyboard-interactive authentication.
Password:
Last login: Fri Sep 28 07:20:31 2012 from 172.16.230.77
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is 'off'.

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

```

- (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.

- 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.

At the prompt, type: **set sensor name <word>**. 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.

- 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**
- 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**

7. 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.

8. If prompted, reboot the Sensor. Type **reboot**

 **Note**

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

9. 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 that the information is correct.
10. 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.

11. Type **show** to verify the configuration information. Check that all information is correct.
12. Type **exit** to exit the session.

:

## Verify successful installation

### Steps:

1. Type **status** in the Sensor CLI. The status report appears.

```

intruShell@ns > status
[Sensor]
System Initialized      : yes
System Health Status   : good
Layer 2 Status         : normal (IDS/IPS)
Installation Status    : complete
IPv6 Status            : Dont Parse and Allow Inline
Reboot Status          : Not Required
Guest Portal Status    : up
Hitless Reboot         : Available
Last Reboot reason     : reboot issued from NSM

[Signature Status]
Present                : yes
Version               : 1.0.0
Power up signature     : good
Geo Location database  : Present
DAT file              : Present
DAT file Version      : 1937.0

[Manager Communications]
Trust Established      : yes (RSA 2048-bit with SHA2 support)
Alert Channel         : up
Log Channel           : up
Authentication Channel : up
Last Error            : None
Alerts Sent           : 344630
Logs Sent             : 208586

[Alerts Detected]
Signature              : 8507809   Alerts Suppressed : 8322935
Scan                  : 3282     Denial of Service : 1113
Malware               : 0

[McAfee MAFD Communication]
Status                : down
IP                    : 0.0.0.0
Port(Secure)         : 8505

```

The Sensor parameter **System Initialized** should be **yes**, and for Manager communication **Trust Established** should be **yes**.

- Return to the Manager. In the Manager Home page, view the Manager status in the System Faults section. The Manager status should be up and Sensor status should be active.

System Faults					
Manager	Status	Critical	Error	Warning	
Manager	Up	1	1	0	
Device	Status	Critical	Error	Warning	
Doc_NS-series_Sensor_1	Active	6	0	3	
Doc_NS-series_Sensor_2	Active	4	1	3	
NS9500_Stack-1	Unknown	0	0	0	
NS9500_Stack-2	Unknown	0	0	0	
NSP_Doc_Sensor_1	Active	0	0	0	
NSP_Doc_Sensor_2	Active	1	0	0	
NSP_Doc_VM600_1	Active	0	0	0	
NSP_Doc_VM600_2	Active	0	0	0	

- From the Manager Home page, click Configure to open the Configuration page.
- Select your added Sensor: Device List → <Device\_Name>. The ports for this Sensor appear under the <Device\_Name> node.

### Note

<Device\_Name> indicates the name of the Sensor you added.

Port	Link	Virtual Adapter	Operation Mode	Placement	Response Port
I/O Module: G0 (2-port QSFP+ module detected)					
0/1	---	---	---	---	---
0/2	---	---	---	---	---
I/O Module: G1 (empty)					
---	---	---	---	---	---
I/O Module: G2 (empty)					
---	---	---	---	---	---
I/O Module: G3 (8-port RJ-45 module detected)					
3/1	⊗ Disabled		In-line Fail Open (Paired with 3/2)	Inside Network	This Port
3/2	⊗ Disabled		In-line Fail Open (Paired with 3/1)	Outside Network	This Port
3/3	⊕ Up		In-line Fail Open (Paired with 3/4)	Inside Network	This Port
3/4	⊕ Up		In-line Fail Open (Paired with 3/3)	Outside Network	This Port
3/5	⊕ Up		In-line Fail Open (Paired with 3/6)	Inside Network	This Port
3/6	⊕ Up		In-line Fail Open (Paired with 3/5)	Outside Network	This Port
3/7	⊗ Disabled		In-line Fail Open (Paired with 3/8)	Inside Network	This Port
3/8	⊗ Disabled		In-line Fail Open (Paired with 3/7)	Outside Network	This Port

- 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 IPS-provided policies, you can clone the policy and then customize it as described in *Trellix Intrusion Prevention System Product Guide*.
- Click Device List → <Device\_Name> → Port Settings.
- 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*.

:

## You're up and running!

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

### Steps:

- For detailed usage instructions, see *Trellix Intrusion Prevention System Product Guide*, or click the ? buttons in the upper-right corner of each window in the Manager.
- Start the Analysis → <Admin Domain> → Attack Log to view alert statistics as attacks are detected. A summary of alerts is displayed in the Unacknowledged Alert Summary monitor of the Manager Dashboard page.
- Having problems? Check *Trellix Intrusion Prevention System Product Guide* for troubleshooting information.

4. 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://supportm.trellix.com>.

:

## Troubleshooting the Sensor

This section lists some common installation problems, the possible causes, and the corresponding solutions.

Problem	Possible Cause	Solution
LED is off.	The Sensor is turned off.	Restore Sensor power.
	The Sensor port cable is disconnected.	Check the Sensor cable connections.
Sensor is operational but is not monitoring traffic.	Network device cables have been disconnected.	Check the cables and make sure they are properly connected to both the network devices and the bypass switch.
	The Sensor ports have not been enabled in the Manager.	The Sensor will not monitor traffic on the ports unless the ports are enabled in the Manager. Ports are disabled in case of Sensor failure; you must re-enable them for Sensor monitoring to resume.
Network or link problems	Improper cabling or port configuration	Make sure that the transmitting and receiving cables are properly connected to the bypass switch.
Runts or giants errors on switch and routers	Improper cabling or port configuration	Make sure that the transmitting and receiving cables are properly connected to the bypass switch.

Problem	Possible Cause	Solution
The critical fault, Switch absent appears in the Manager System faults page.	The fail-open kit is disconnected.	Check the fail-open kit and make sure it is properly connected to the Sensor.

For more information on troubleshooting steps and faults generated in the Manager, see the *Troubleshooting* section in *Trellix Intrusion Prevention System Product Guide*.

:

## Sensor technical specifications

The following table lists the specifications of an NS5x00 Sensor:

Sensor Specifics	NS5200	NS5100
Dimensions	1RU Rack Mountable 17.25" (W) x 1.75" (H) x 24.625" (D)	1RU Rack Mountable 17.25" (W) x 1.75" (H) x 24.625" (D)
Weight	22 lbs.	22 lbs.
Storage	Solid State 80 GB	Solid State 80 GB
<b>System Heat Dissipation</b>		
Maximum BTU	767	767
Typical BTU	512	512
Maximum Power Consumption	225W	225W
Redundant Power Supply	Included	Included
Power	100-240 VAC (50/60Hz)	

---

Sensor Specifics	NS5200	NS5100
Temperature	Operating: 0°-35° C , Non-operating: - 40° - 70° C	
Relative humidity (non-condensing)	Operational: 10% -90%, Non-operational: 5% -95%	
Altitude	0 to 10,000 feet	
Safety Certification	UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB license and report covering all national country deviations.	
EMI Certification	FCC Part 15, Class A (CFR 47) (USA) ICES-003 Class A (Canada), EN55022 Class A (Europe), CISPR22 Class A (Int'l)	

:

## NS3500 Sensors

:

### About Sensors

Sensors are high-performance, scalable, and flexible content processing appliances built for accurate detection and prevention of:

- Network intrusions
- Network misuse
- Distributed Denial-of-Service (DDoS) attacks

Sensors are specifically designed to handle traffic at wire speed, efficiently inspect and detect intrusions with a high degree of accuracy, and are flexible enough to adapt to the security needs of any enterprise environment. When deployed at key network access points, the Sensor provides real-time traffic monitoring to detect malicious activity and respond to such activity based on the responses configured by the administrator.

After you deploy a Sensor successfully, you configure and manage it using the Manager. The process of configuring a Sensor and establishing communication with the Manager is described in the subsequent chapters of this guide. For details about the Manager, see the *Manager Administration* section in *Trellix Intrusion Prevention System Product Guide*.

:

### Functions of NS-series Sensors

The NS-series Sensors are a third-generation hardware platform Sensors designed for high bandwidth links to offer Next Generation IPS (NGIPS) capability and provide high aggregate throughput across various Sensor models. The NS3500 model has a throughput of 750 Mbps.

The primary function of a Sensor is to analyze traffic on selected network segments and to respond when an attack is detected. The Sensor examines the header and data portions of every network packet, looking for patterns and behavior in the network traffic that indicate malicious activity. The Sensor examines packets according to user-configured policies, or rule sets, which determine what attacks to watch for, and how to respond with countermeasures if such an attack is detected.

If an attack is detected, a Sensor responds according to its configured policy. The Sensor can perform many types of attack responses, including generating alerts and packet logs, resetting TCP connections, "scrubbing" malicious packets, and even blocking attack packets entirely before they reach the intended target.

:

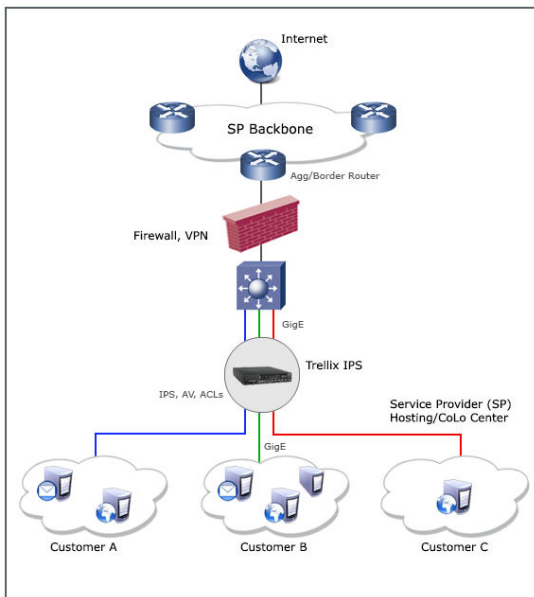
### Deployment of NS-series Sensors



Deployment of a Sensor requires knowledge of your network to help determine the level of configuration and the number of installed Sensors. The Sensor is purpose-built to monitor traffic across one or more network segments.

Following is an example of a network topology using Gigabit Ethernet throughput. In the illustration, Trellix Intrusion Prevention System provides IPS protection to outsourced servers. High port-density and virtualization provides a highly scalable solution, while Trellix IPS protects against web and eCommerce mail server exploits.

A sample NS-Series Sensor deployment



:

## NS3500 Sensor physical description

The high-port density NS-series Sensor is designed for high bandwidth links. This section gives a physical description of the NS3500 Sensors.

The NS3500 Sensor model provide 750 Mbps throughput.

:

### Components of an NS3500 Sensor

The NS3500 front and rear panel details are described below.

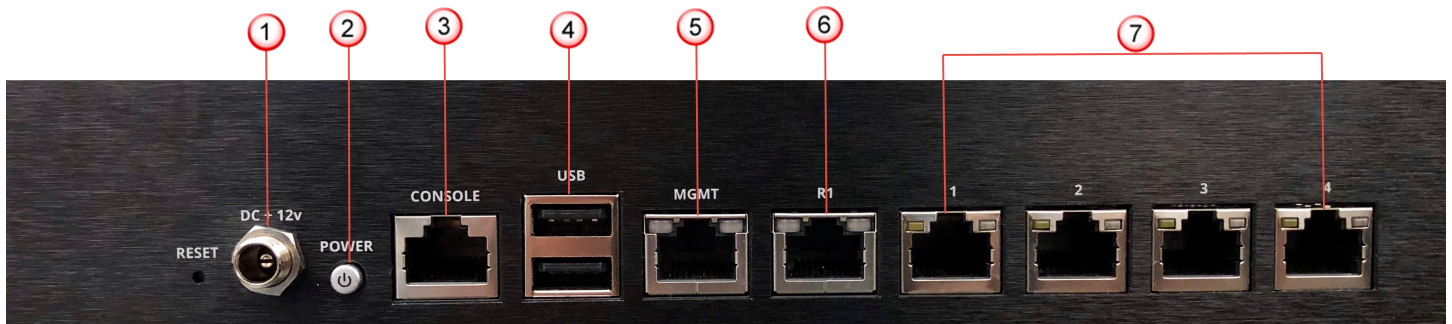
## The NS3500 Sensor model

### Sensor front panel



1. Power LED
2. Status LED
3. Compact Flash Memory LED
4. Speed LED for each ethernet port
5. Link LED for each ethernet port

### Sensor rear panel



1. Power supply (12V DC IN)
2. Power switch
3. RJ-45 Console port (1)
4. USB ports (2)
5. RJ-45 10/100/1000 Management port (MGMT) (1)
6. RJ-45 10/100/1000 Response port (R1) (1 - currently not supported)
7. RJ-45 10/100/1000 Mbps Ethernet Monitoring ports (4)

The following table gives the details of the supported ports.

Ports	NS3500
Fixed RJ-45 ports (internal fail-open)	4 (10/100/1000 Mbps)
Console port	1
Dedicated Management ports (RJ-45)	1 (10/100/1000 Mbps)
USB port	2

- **Console port** — Use to set up and configure the Sensor using the CLI.
- **RJ-45 10/100/1000 Mbps ethernet monitoring ports** — Enables you to monitor four SPAN ports, two segments in-line, or a combination
- **External USB port** — Use these in troubleshooting situations for system recovery purposes. You need to restart the Sensor through the USB storage device.
- **RJ-45 10/100/1000 Management port** — Use for communication with the Manager server. You can assign an IP address to this port during installation.
- **Power Supply** — Power supply is included with an NS3500 Sensor. The supply uses a 12V DC IN. Trellix provides 12V DC adapter with power cord. International customers must procure a country-appropriate power cable.

The NS-series Sensor does not have internal taps; you must use it with a third-party external tap to run it in tap mode.

:

## Sensor LEDs

The front panel LEDs provide status information for the health of the Sensor and the activity on its ports.

### Front panel LEDs

LED	Status	Description
Power	Green Off	Power supply is functioning. Power supply is not functioning or the unit has no power feed.
Status	Green Off	It indicates that Sensor is in good health.

LED	Status	Description
		System is booting up or one of the parameters/operations is not in good health status.
Hard drive	Blinking Amber Off	Hard drive is operational. Hard drive is not operational.
Management Port Speed	Amber Green Off	The port speed is 1000 Mbps. The port speed is 100 Mbps. The port speed is 10 Mbps.
Management Port Link	Amber Blinking Amber	The link is up. Data is being received or transmitted.
Ethernet Ports Speed	Amber Green Off	The port speed is 1000 Mbps. The port speed is 100 Mbps. The port speed is 10 Mbps.
Ethernet Ports Link	Amber Blinking Amber	The link is up. Data is being received or transmitted.

### Back panel LEDs

LED	Status	Description
Management Port Speed	Amber Green Off	The port speed is 1000 Mbps. The port speed is 100 Mbps. The port speed is 10 Mbps.
Management Port Link	Amber Blinking Amber	The link is up. Data is being received or transmitted.

LED	Status	Description
Ethernet Ports Speed	Amber Green Off	The port speed is 1000 Mbps. The port speed is 100 Mbps. The port speed is 10 Mbps.
Ethernet Ports Link	Amber Blinking Amber	The link is up. Data is being received or transmitted.

:

## Before you install

This chapter describes best practices for deployment of Sensors in your network. Topics include safety considerations for handling the Sensor, usage restrictions that apply to the Sensor model, and contents that are shipped along with the Sensor.

:

### Usage restrictions

The following restrictions apply to the use and operation of a Sensor:

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

:

### Safety measures

Please read the following warnings before you install the Sensor. These safety measures apply to all Sensor models unless otherwise noted. Failure to observe these safety warnings could result in serious physical injury.

### Warnings

- Read the installation instructions before you connect the system to its power source.
- To remove all power from the Sensor, unplug all power cords.
- Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

- Before working on the equipment that is connected to power lines, remove all jewelry including rings, necklaces, and watches. Metal objects will heat up when connected to power and ground, and can cause serious burns or weld the metal object to the terminals.
- This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.
- To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Exercise caution when connecting cables.
- This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the users will be required to correct the interference at their own expense.
- Refer to the Appendix for information on regulatory, compliance, and other safety requirements.

:

### Contents of the box

The following accessories are shipped in the NS3500 Sensor crate:

- Sensor
- 12V DC adapter with power cord
- Printed Quick Start Guide
- RJ45 to DB9 console cable
- Set of rack mounting ears with screws
- Set of rubber feet (4x)The set of rubber feet can be used if the Sensor is placed in a desktop setting.

:

### Unpack the Sensor

Steps:

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

:

## Setting up the Sensor

This chapter describes how to set up the Sensor for you to configure it.

:

### Setup overview

Setting up a Sensor involves the following steps:

1. Position the Sensor as described in the section [How to position the Sensor](#).
2. Attach power, network, and monitoring cables.
3. Turn on the Sensor.
4. Configure the Sensor after you have set up and turned it on.

:

### How to position the Sensor

Place the Sensor in a physically secure location, close to the switches or routers it will be monitoring. Ideally, the Sensor must be located within a standard communications rack. To mount the Sensor on a rack, install the Sensor as described in the subsequent sections of this guide.

:

## Attaching cables to the Sensor

Follow the steps outlined in this chapter to connect the cables to the various ports of your Sensor.

:

### Connect the cable to the Console port

The Console port on the NS3500 Sensor is used for setup and configuration of the Sensor.

**Steps:**

1. For console connections, plug in the RJ-45 cable supplied by Trellix into the Console port on the Sensor. This port is labeled **CONSOLE** in the Sensor front panel.



2. Connect the other end of the Console port cable directly to a COM port of the computer or terminal server you will use to configure the Sensor, for example, a computer 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. Required settings for HyperTerminal are listed below:

Name	Setting
Baud rate	115200
Number of bits	8
Parity	None
Stop bits	1
Flow control	None

3. Turn on the Sensor.

:

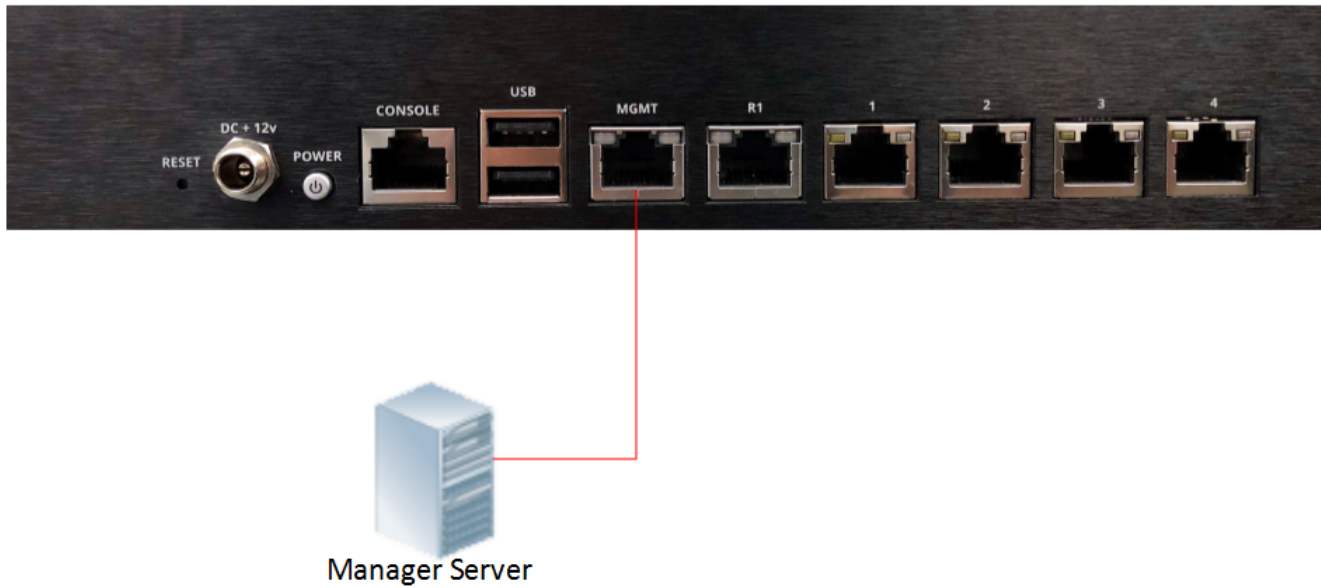
### Connect the cable to the Management port

The Sensor communicates with the Manager using the Management port.

#### Steps:

1. Plug a RJ-45 cable into the Management port. This port is labeled **MGMT** in the front panel of the NS3500 Sensor.





2. Plug the other end of the cable into the network device connected to your Manager server.

#### Note

To isolate and protect your management traffic, Trellix strongly recommends you to use a separate, dedicated management subnet to interconnect the Sensors and the Manager.

:

### About connecting cables to the Monitoring ports

Connect to network devices that will send traffic to the Sensor monitoring ports. You can deploy Sensors in the following operating modes:

- Inline Fail Closed
- SPAN or Hub
- Tap

#### Note

Only internal Fail-Open is available for NS3500 Sensors.

:

### Cable types for routers, switches, hubs, and computers

This section lists the types of cables that you require to connect the Sensor to other network devices:

- Use a crossover Ethernet RJ-45 cable to connect a router port to the monitoring ports.
- Use a straight-through Ethernet RJ-45 cable to connect a switch or a hub port to monitoring ports.
- Use a crossover Ethernet RJ-45 cable to connect a router port to computer to the Sensor monitoring port.
- Use a crossover Ethernet RJ-45 cable to connect a computer to the Sensor monitoring port.

:

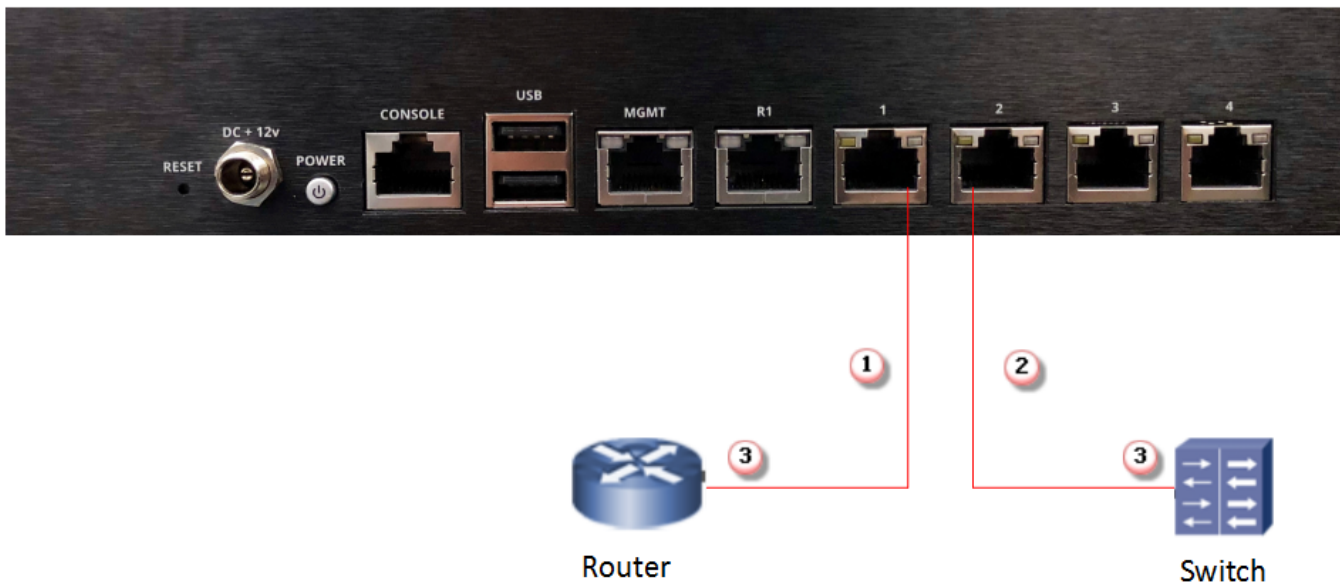
## Connect the cables for in-line mode

In-line ethernet ports can be configured as fail-open or fail-closed. The RJ-45 monitoring ports are built-in and include an built-in fail-open functionality as well.

Ethernet ports fail-close, implying that the flow of traffic will stop if the Sensor fails. To allow traffic to flow uninterrupted, you must use special hardware, and cable the Sensor to external active fail-open kits. For instructions, see the subsequent sections of this chapter.

This section provides steps to connect the Sensor's ethernet ports so they fail-close.

1. Plug the cable into one of the monitoring ports, for example 1.
2. Plug the cable into the other monitoring port, for example 2.




3. 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 and the one connected to 2 to the switch.

:

## Connect the cables for tap mode

To deploy the Sensor in tap mode, you must use a Sensor's ethernet monitoring port pair with a third-party external tap.

 **Note**

For a list of Trellix-approved third party vendors, see the KnowledgeBase at <https://supportm.trellix.com>. Enter the relevant KnowledgeBase article in Search the Support Knowledge Center and click Search to locate the relevant KnowledgeBase article.

**Steps:**

1. Plug the ethernet cable into one of the monitoring ports, for example, port 3.
2. Plug the cable into one of the monitoring ports labeled 4.
3. Connect the other end of each cable to the tap.
4. Connect the network devices that you want to monitor to the tap.

:

## Connect the cables for SPAN or hub mode

For the Sensor, monitoring in SPAN or hub mode occurs in in-line fail-open mode. When you monitor in SPAN or hub mode, you use single ports.

To connect a Sensor to a SPAN port or hub, plug an RJ-45 cable into one of the port and connect the other end of the cable to the SPAN port or the hub.

:

## Turning the Sensor on and off

 **Note**

Do not attempt to turn on the Sensor until you have installed the Sensor in a rack and made all the necessary network connections.

**Steps:**

1. Connect the power cable to the Sensor power inlet.
2. Connect the power cable to a power source. Trellix recommends that you use the **shutdown** CLI command to halt the Sensor before turning it off. For more information on CLI commands, see the *CLI commands* section in *Trellix Intrusion Prevention System Product Guide*.
3. Press the power button to turn on the Sensor.

:

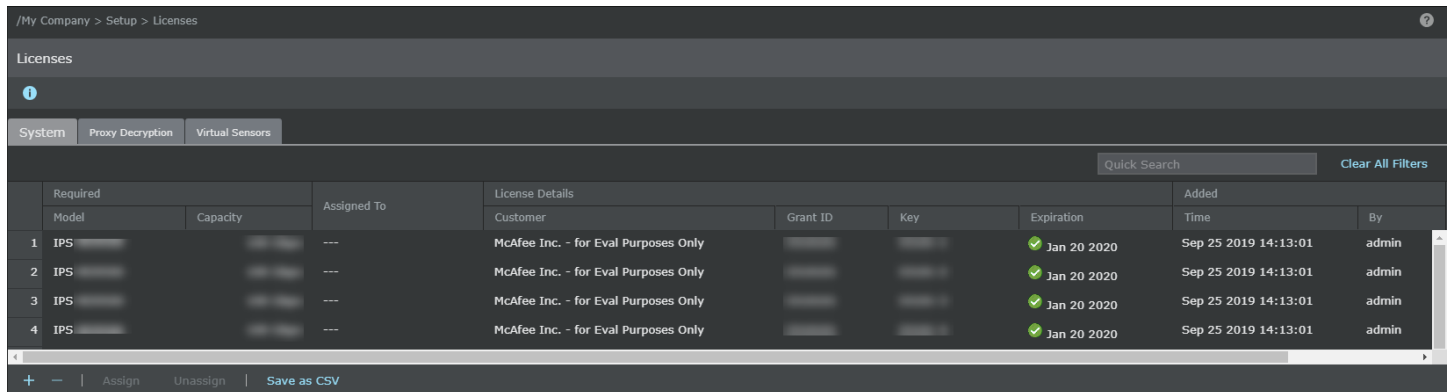
## Managing licenses for NS3500 Sensors

The NS3500 Sensors require a software license to activate the baseline throughput of 750 Mbps on NS3500 Sensors. The license is provided as a .zip or .jar file. The Manager supports both formats. The license procured contains the details for the throughput for the Sensors.

### Note



You must first purchase a license to enable traffic inspection in NS3500 Sensor. To obtain a license, contact Trellix Sales.


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



	Required		Assigned To	License Details				Added	
	Model	Capacity		Customer	Grant ID	Key	Expiration	Time	By
1	IPS		---	McAfee Inc. - for Eval Purposes Only			Jan 20 2020	Sep 25 2019 14:13:01	admin
2	IPS		---	McAfee Inc. - for Eval Purposes Only			Jan 20 2020	Sep 25 2019 14:13:01	admin
3	IPS		---	McAfee Inc. - for Eval Purposes Only			Jan 20 2020	Sep 25 2019 14:13:01	admin
4	IPS		---	McAfee Inc. - for Eval Purposes Only			Jan 20 2020	Sep 25 2019 14:13:01	admin

The following details are displayed on the System tab:

Option	Definition
Required	Model – Sensor model compatible with the license Capacity – Throughput limit for the license
Assigned To	Name of the Sensor assigned to the license.
License Details	Customer – Customer for whom the license file was generated Grant ID – Trellix Grant ID of the corresponding customer Key – License key number of the customer Expiration – Applicable only for demo and subscription licenses <ul style="list-style-type: none"> <li>•  : Valid license</li> <li>•  : Expired license</li> </ul>

Option	Definition
	Type – Displays if the license is Perpetual, Subscription, or Evaluation (Demo) type. <div data-bbox="769 394 1357 554" style="background-color: #e0f2f7; padding: 5px; margin-top: 10px;">  <b>Note:</b>              It is recommended to install subscription license from Manager version 10.1.7.44 and later.           </div>
Added	Time – Date in <mmm-yy> format, and time when the license was added By – Name of the user who added the license
Comments	Enables you to add your comment per license file that is imported. Double-click in the Comment field and enter your comment. Click outside this field and your comment is automatically saved.


The following actions can be performed on the System tab:

- [Add a license](#)
- [Assign a license to a Sensor](#)
- [Unassign a license from a Sensor](#)
- [Remove a license](#)
- [Export the license list in CSV format](#)

:

## Add license to the Manager

To upload the license, perform the following steps:

1. Go to Manager → <Admin Domain Name> → Setup → Licenses.
2. Click the System tab.
3. Click .

The Add License pop-up window opens.

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

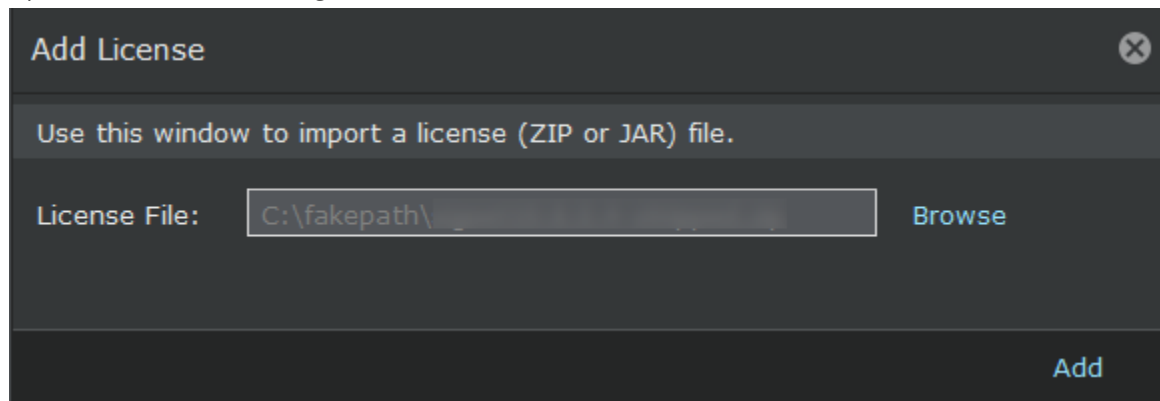
 **Note**

The supported license formats are .zip and .jar.

 **Note**

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

Upload license to the Manager



5. Click Add.

The license is uploaded to the Manager.

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

:

## Assign a license to a Sensor

To assign the license, perform the following steps:

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

/My Company > Setup > Licenses

Licenses

System Proxy Decryption Virtual Sensors

Quick Search Clear All Filters

	Required		Assigned To	License Details					Added
	Model	Capacity		Customer	Grant ID	Key	Expiration ↑	Type	
1	IPS-NS3500	750 Mbps	---				---	Perpetual	Dec 16 2023
2	IPS-NS3500	750 Mbps	---				---	Perpetual	Dec 16 2023
3	IPS-NS3500	750 Mbps	---				---	Perpetual	Dec 16 2023
4	IPS-NS3500	750 Mbps	---				---	Perpetual	Dec 16 2023
5	IPS-NS3500	750 Mbps	---				---	Perpetual	Dec 16 2023
6	IPS-NS3500	750 Mbps	---				---	Perpetual	Dec 16 2023
7	IPS-NS3500	750 Mbps	---				---	Perpetual	Dec 16 2023
8	IPS-NS3500	750 Mbps	---				---	Perpetual	Dec 16 2023

+ - | Assign Unassign | Save as CSV 20 licenses

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

Assign License

Model: IPS-NS3500

Capacity: 750 Mbps

Grant ID: [Redacted]

Key: [Redacted]

Expiration: Dec 31 2030

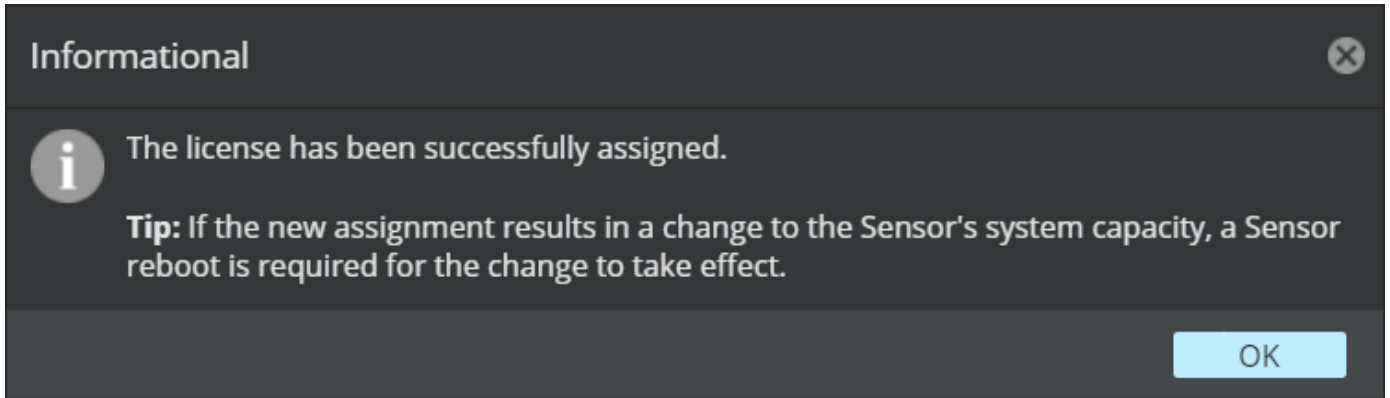
Assign To: /My Company/NS3500\_84

Assign

### Note

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

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



### Note

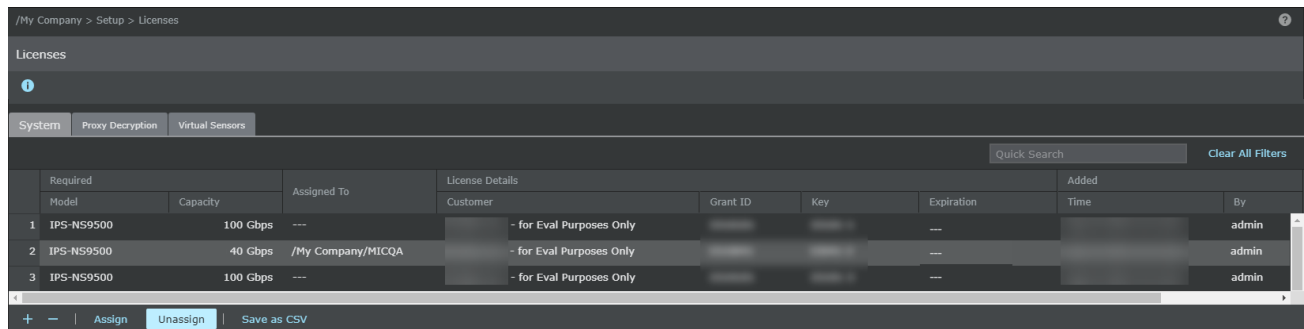
You must reboot the device for the changes to take effect.

:

## Unassign a license from a Sensor

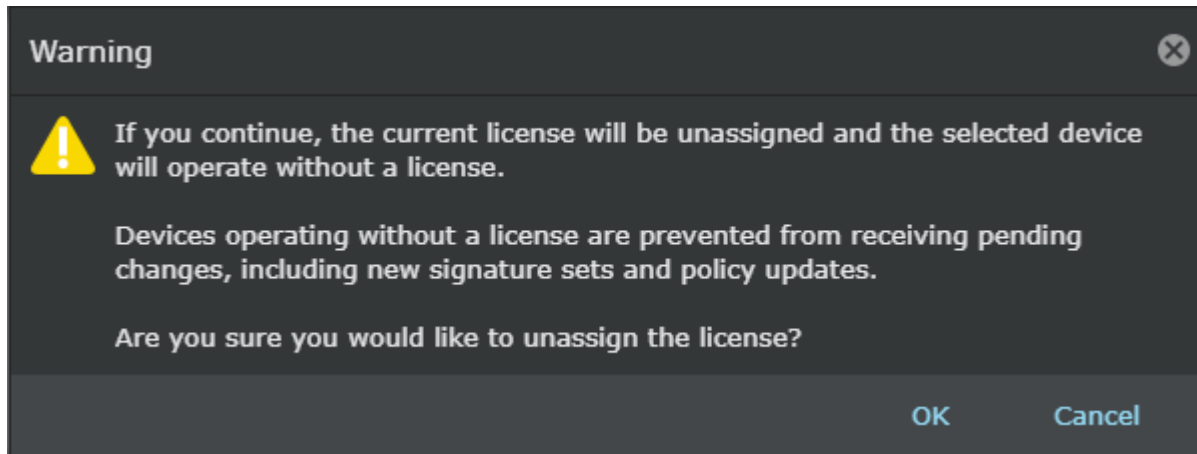
To unassign the license, perform the following steps:

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



4. Click Unassign.
5. Click Ok.






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

:

## Remove a license from the Manager

To remove a license, perform the following steps:

### Steps:

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

:

## Troubleshooting the Sensor

This section lists some common installation problems, the possible causes, and the corresponding solutions.

Problem	Possible Cause	Solution
LED is off.	The Sensor is turned off.	Restore Sensor power.

Problem	Possible Cause	Solution
	The Sensor port cable is disconnected.	Check the Sensor cable connections.
Sensor is operational but is not monitoring traffic.	Network device cables have been disconnected.	Check the cables and make sure they are properly connected to both the network devices and the bypass switch.
	The Sensor ports have not been enabled in the Manager.	The Sensor will not monitor traffic on the ports unless the ports are enabled in the Manager. Ports are disabled in case of Sensor failure; you must re-enable them for Sensor monitoring to resume.
Network or link problems	Improper cabling or port configuration	Make sure that the transmitting and receiving cables are properly connected to the bypass switch.
Runts or giants errors on switch and routers	Improper cabling or port configuration	Make sure that the transmitting and receiving cables are properly connected to the bypass switch.
The critical fault, Switch absent appears in the Manager System faults page.	The fail-open kit is disconnected.	Check the fail-open kit and make sure it is properly connected to the Sensor.

For more information on troubleshooting steps and faults generated in the Manager, see the *Troubleshooting* section in *Trellix Intrusion Prevention System Product Guide*.

:

## Sensor technical specifications

The following table lists the specifications of an NS3500 Sensor:

<b>Sensor Specifics</b>	<b>NS3500</b>
<b>Dimensions</b>	1RU Rack Mountable 9.45" (W) x 1.73" (H) x 6.54" (D)
<b>Weight</b>	2.65 lbs.
<b>Storage</b>	Compact Flash Memory Card 32GB
<b>System Heat Dissipation</b>	
<b>Maximum BTU</b>	102
<b>Typical BTU</b>	61
<b>Maximum Power Consumption</b>	30W
<b>Power</b>	100 -240 VAC (50-60Hz)
<b>Temperature</b>	Operating: 0° to 35° C , Non-operating: -40° to 70° C
<b>Relative humidity (non-condensing)</b>	Operational: 10% to 90%, Non-operational: 5% to 95%
<b>Altitude</b>	0 to 10,000 feet
<b>Safety Certification</b>	UL 60950-1 (USA); CSA 22.1.No. 60950-1 (Canada); EN 60950-1 (Europe); CNS 14336-1 (Taiwan); GB 4943-1 and GB 17625.1 (China) IEC 60950-1 (International)-CB Scheme certificate and test report covering all applicable country deviations
<b>EMI Certification</b>	FCC Part 15 Subpart B Class B (USA); CAN ICES-3 Class B (Canada); EN 55022, EN 55032,

---

Sensor Specifics	NS3500
	EN 55024, EN61000-3-2, EN61000-3-3 (Europe and International) KN32 and KN35 (South Korea); VCCI Class B (Japan); AS/NZS CISPR 32 (Australia and New Zealand); CNS 13438 (Taiwan); GB 9254-2008 (China)

:

## NS3x00 Sensors

:

### About Sensors

Sensors are high-performance, scalable, and flexible content processing appliances built for the accurate detection and prevention of:

- Network intrusions
- Network misuse
- Distributed Denial-of-Service (DDoS) attacks

These Sensors are specifically designed to handle traffic at wire speed, efficiently inspect and detect intrusions with a high degree of accuracy, and are flexible enough to adapt to the security needs of any enterprise environment. When deployed at key network access points, the Sensor provides real-time traffic monitoring to detect malicious activity and respond to such activity based on the responses configured by the administrator.

After you deploy a Sensor successfully, you configure and manage it using the Manager. The process of configuring a Sensor and establishing communication with the Manager is described in the subsequent chapters of this guide. For the details about the Manager, see the *Manager Administration* section in *Trellix Intrusion Prevention System Product Guide*.

:

### Functions of NS-series Sensors

The NS-series Sensors are a third-generation hardware platform Sensor designed for high bandwidth links to offer Next Generation IPS (NGIPS) capability and provide high aggregate throughput across various Sensor models. The following models are supported.

- NS3200 - The NS3200 Sensor is a 1RU device providing an aggregate throughput of 750 Mbps
- NS3100 - The NS3100 Sensor is a 1RU device providing an aggregate throughput of 750 Mbps

The primary function of a Sensor is to analyze traffic on selected network segments and to respond when an attack is detected. The Sensor examines the header and data portions of every network packet, looking for patterns and behavior in the network traffic that indicate malicious activity. The Sensor examines packets according to user-configured policies, or rule sets, which determine what attacks to watch for, and how to respond with countermeasures if such an attack is detected.

If an attack is detected, a Sensor responds according to its configured policy. The Sensor can perform many types of attack responses, including generating alerts and packet logs, resetting TCP connections, "scrubbing" malicious packets, and even blocking attack packets entirely before they reach the intended target.

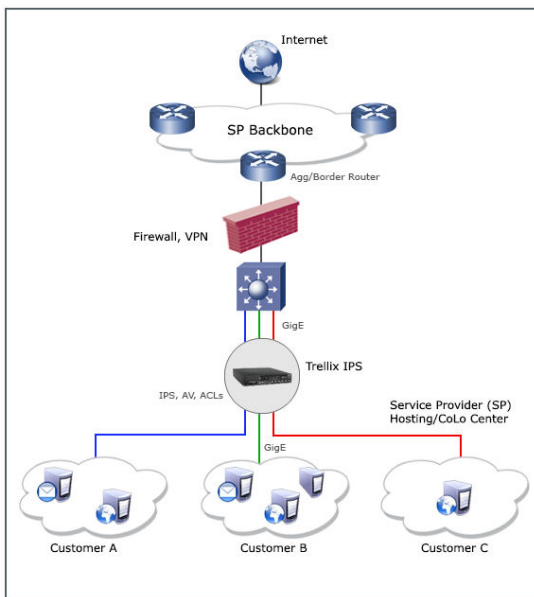
:

## Deployment of NS-series Sensors

Deployment of a Sensor requires knowledge of your network to help determine the level of configuration and the number of installed Sensors. You also need to determine the number of Trellix ePolicy Orchestrator - On-prem servers required to protect your network. The Sensor is purpose-built to monitor traffic across one or more network segments.

Following is an example of a network topology using Gigabit Ethernet throughput. In the illustration, Trellix Intrusion Prevention System provides IPS protection to outsourced servers. High port-density and virtualization provides a highly scalable solution, while Trellix IPS protects against web and eCommerce mail server exploits.

### A sample NS-Series Sensor deployment



:

## NS3x00 Sensor physical description

The high-port density NS-series Sensor is designed for high bandwidth links. This section gives a physical description of the NS3x00 Sensors.

The NS3200 and NS3100 Sensor models provide 750 Mbps throughput.

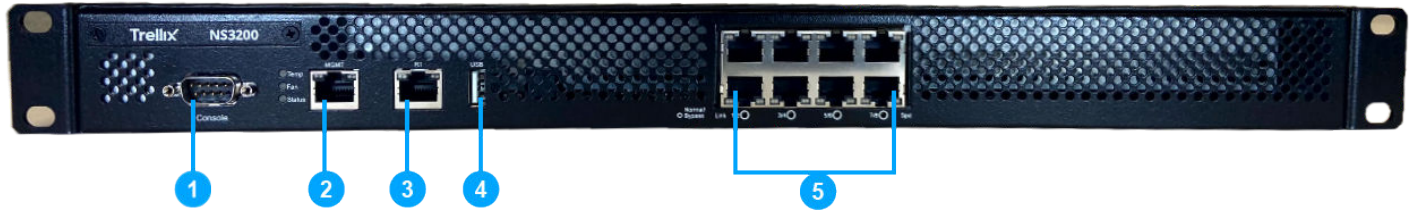
:

### Components of an NS3x00 Sensor

The NS3x00 front and rear panel details are described below.

## The NS3100/NS3200 Sensor model

### Sensor front panel



1. Console port (1)
2. RJ-45 10/100/1000 Management port (MGMT) (1)
3. RJ-45 10/100/1000 Response port (R1) (1)
4. USB port (1)
5. RJ-45 10/100/1000 Mbps Ethernet Monitoring ports (8)

### Sensor rear panel



1. Power supply inlet (1)
2. Fan units (3)

The direction of airflow in all the Sensors is from front to back. Cold air enters through the front of the chassis.

The following table gives the details of the supported ports.

Ports	NS3100/NS3200
Fixed RJ-45 ports (internal fail-open)	8 (10/100/1000 Mbps)
Console port	1
Dedicated Response ports (RJ-45)	1 (10/100/1000 Mbps)

Ports	NS3100/NS3200
Dedicated Management ports (RJ-45)	1 (10/100/1000 Mbps)
USB port	1

- **Console port** — Use to set up and configure the Sensor using the CLI.
- **RJ-45 10/100/1000 Mbps ethernet monitoring ports** — Enables you to monitor eight SPAN ports, four segments in-line, or a combination
- **External USB port** — Use these in troubleshooting situations for system recovery purposes. You need to restart the Sensor through the USB storage device.
- **RJ-45 10/100/1000 Management port** — Use for communication with the Manager server. You can assign an IP address to this port during installation.
- **RJ-45 10/100/1000 Response port** — When you operate this port in SPAN or tap mode, it enables you to inject response packets back through a switch or a router.
- **Power Supply** — Power supply is included with an NS3x00 Sensor. The supply uses a standard IEC port (IEC320-C13). Trellix provides a standard, 2 m NEMA 5-15P (US) power cable (3 wire). International customers must procure a country-appropriate power cable.

The NS-series Sensor does not have internal taps; you must use it with a third-party external tap to run it in tapped mode.

:

## Sensor LEDs

The front panel LEDs provide status information for the health of the Sensor and the activity on its ports.

### Front panel LEDs

LED	Status	Description
Temp	Green Amber	Inlet air temperature measured inside the chassis is normal. (Chassis temperature OK) Inlet air temperature measured inside the chassis is too high. (Chassis temperature too hot)
Fan	Green	All the fans are operating.



LED	Status	Description
	Amber	One or more fans are not working.
Status	Green Amber	It indicates that Sensor is in good health. System is booting up or something is not in good health status.
Management Port Speed	Green Amber Off	The port speed is 1000 Mbps. The port speed is 100 Mbps. The port speed is 10 Mbps.
Management Port Link	Green Off	The link is up. The link is down.
Response Port Speed	Green Amber Off	The port speed is 1000 Mbps. The port speed is 100 Mbps. The port speed is 10 Mbps.
Response Port Link	Green Off	The link is up. The link is down.
Normal/Bypass	Green Off	The port pair is in Inline Fail-Open/Inline Fail-Close/SPAN/Tap Mode. The Port Pair is in the Bypass Mode.
Ethernet Ports Link	Green Off	The link is up. The link is down.
Ethernet Ports Speed	Green Amber Off	The port speed is 1000 Mbps. The port speed is 100 Mbps. The port speed is 10 Mbps.

 **Note**

There are no rear panel LEDs on the NS3x00 Sensors.

:

## Before you install

This chapter describes best practices for deployment of Sensors in your network. Topics include safety considerations for handling the Sensor, usage restrictions that apply to the Sensor model, and contents that are shipped along with the Sensor.

:

### Usage restrictions

The following restrictions apply to the use and operation of a Sensor:

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

:

### Safety measures

Please read the following warnings before you install the Sensor. These safety measures apply to all Sensor models unless otherwise noted. Failure to observe these safety warnings could result in serious physical injury.

#### Warnings:

- Read the installation instructions before you connect the system to its power source.
- To remove all power from the Sensor, unplug all power cords.
- Only trained and qualified personnel should be allowed to install, replace, or service this equipment.
- Before working on the equipment that is connected to power lines, remove all jewelry including rings, necklaces, and watches. Metal objects will heat up when connected to power and ground, and can cause serious burns or weld the metal object to the terminals.
- This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.
- To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Exercise caution when connecting cables.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the

equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, might cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the users will be required to correct the interference at their own expense.

- Refer to the Appendix for information on regulatory, compliance, and other safety requirements.

:

## Contents of the box

The following accessories are shipped in the NS3x00 Sensor crate:

- Sensor
- Power cords (Trellix provides a standard and international power cables)
- Printed Quick Start Guide

:

## Unpack the Sensor

Steps:

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

:

## Setting up the Sensor

This chapter describes how to set up the Sensor for you to configure it.

:

### Setup overview

Setting up a Sensor involves these steps:

1. Position the Sensor as described in the section [How to position the Sensor](#).
2. Attach power, network, and monitoring cables.
3. Turn on the Sensor.
4. Configure the Sensor after you have set up and turned it on.

:

### How to position the Sensor

Place the Sensor in a physically secure location, close to the switches or routers it will be monitoring. Ideally, the Sensor must be located within a standard communications rack. To mount the Sensor on a rack, install the Sensor as described in the subsequent sections of this guide.

:

### Install the Sensor

Trellix recommends rack-mounting your Sensor. The mounting ears are pre-attached to the Sensor. For maintenance purposes, you must have access to the front and rear of the Sensor.

#### Caution

Before you mount the Sensor on the rack, make sure that the power is off. Remove the power cable and all network interface cables from the Sensor.

#### Important

Due to the weight of the appliance, Trellix recommends that one person holds the chassis and the other person fixes it to the rail cabinet.

Install the Sensor into a rack.



:

## Attaching cables to the Sensor

Follow the steps outlined in this chapter to connect the cables to the various ports of your Sensor.

:

### Connect the cable to the Console port

The Console port on the NS3x00 Sensor is used for setup and configuration of the Sensor.

#### Steps:

1. For console connections, plug in the DB9 Console cable supplied by Trellix into the Console port on the Sensor. This port is labeled **Console** in the Sensor front panel.



2. Connect the other end of the Console port cable directly to a COM port of the computer or terminal server you will use to configure the Sensor, for example, a computer 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. Required settings for HyperTerminal are listed below:

Name	Setting
Baud rate	115200
Number of bits	8
Parity	None
Stop bits	1
Flow control	None

3. Turn on the Sensor.

:

### Connect the cable to the Response port

While operating in tap or SPAN mode, the Sensor uses its Response port to respond to attacks. When deployed in tap mode, the Sensor does not inject response packets through the tap but uses the Response port.

#### Steps:

1. Plug a Cat-5e Ethernet cable into the Response port. This port is labeled **R1** on the Sensor rear panel.
2. Connect the other end of the cable to the network device such as a hub, switch, or router, through which you want the Sensor to respond to attacks.

:

### Connect the cable to the Management port

The Sensor communicates with the Manager using the Management port.

#### Steps:

1. Plug a Category 5e or 6a Ethernet cable into the Management port. This port is labeled **MGMT** in the front panel of the NS3x00 Sensor.



2. Plug the other end of the cable into the network device connected to your Manager server.

### Note

To isolate and protect your management traffic, Trellix strongly recommends using a separate, dedicated management subnet to interconnect the Sensors and the Manager.

:

## About connecting cables to the Monitoring ports

Connect to network devices that will send traffic to the Sensor monitoring ports. You can deploy Sensors in the following operating modes:

- Inline Fail Open
- Inline Fail Open – Active
- Inline Fail Closed
- SPAN or Hub
- Tap

:

## How to use peer ports

You must use two peer monitoring ports of the Sensor to deploy it in full duplex mode. The Sensor's numbered ports are internally wired in pairs to accommodate the traffic.

The following ethernet ports are coupled and must be used together.

Port Pairs	Sensor
1 and 2	NS3200/NS3100
3 and 4	NS3200/NS3100

Port Pairs	Sensor
5 and 6	NS3200/NS3100
7 and 8	NS3200/NS3100

### Note

Since monitoring ports are internally wired, when you disable one of the ports in a pair, the corresponding port is also disabled.

:

## Cable types for routers, switches, hubs, and computers

This section lists the types of cables that you require to connect the Sensor to other network devices:

- Use a crossover Ethernet RJ-45 cable to connect a router port to the monitoring ports.
- Use a straight-through Ethernet RJ-45 cable to connect a switch or a hub port to monitoring ports.
- Use a crossover Ethernet RJ-45 cable to connect a router port to the computer to the Sensor Management port.
- Use a crossover Ethernet RJ-45 cable to connect a computer to the Sensor monitoring port.

:

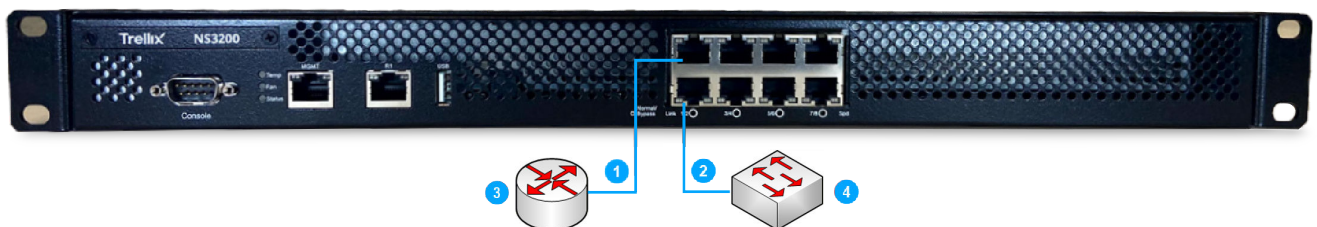
## Connect the cables for in-line mode

In-line ethernet ports can be configured as fail-open or fail-closed. The RJ-45 monitoring ports are built-in and have a fail-open function built-in as well.

Ethernet ports fail-close, implying that the flow of traffic will stop if the Sensor fails. To allow traffic to flow uninterrupted, you must use special hardware, and cable the Sensor to external active fail-open kits. For instructions, see the subsequent sections of this chapter.

This section provides steps to connect the Sensor's ethernet ports so they fail-close.

1. Plug the cable into one of the monitoring ports, for example 1.
2. Plug the cable into the other monitoring port, for example 2.





3. 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).

:

## Connect the cables for tap mode

To deploy the Sensor in tap mode, you must use a Sensor's ethernet monitoring port pair with a third-party external tap.

### Note

For a list of Trellix-approved third party vendors, see the KnowledgeBase at <https://supportm.trellix.com>. Enter the relevant KnowledgeBase article in Search the Support Knowledge Center and click Search to locate the relevant KnowledgeBase article.

#### Steps:

1. Plug the ethernet cable into one of the monitoring ports, for example, port 3.
2. Plug the cable into one of the monitoring ports labeled 4.
3. Connect the other end of each cable to the tap.
4. Connect the network devices that you want to monitor to the tap.

:

## Connect the cables for SPAN or hub mode

For the Sensor, monitoring in SPAN or hub mode occurs in in-line fail-open mode. When you monitor in SPAN or hub mode, you use only single ports.

To connect an Sensor to a SPAN port or hub, plug an RJ-45 cable into one of the port and connect the other end of the cable to the SPAN port or the hub.

:

## Connect the cables for Sensor Fail-Open

Fail-Open kits minimize the potential risks of in-line Sensor failure on critical network links. You need to purchase these kits separately. Copper versions of the kit are available for the one-gigabit ports.

Monitoring ports of the Sensors can be fail-close; thus, if the Sensor is deployed in-line fail-close, a hardware failure results in network downtime except the built-in RJ-45 ports which come with built-in fail-open functionality.

While the Sensor is operating, the active fail-open kit is in-line and routes all traffic directly through the Sensor. When the Sensor fails, the fail-open switch automatically shifts to a bypass state; in-line traffic continues to flow through the network link but is no

longer routed through the Sensor. After the Sensor resumes normal operation, the switch returns to the in-line state, enabling in-line monitoring.

The NS3x00 Sensors have built-in RJ-45 ports with fail-open and support active fail-open when connected to an active fail-open kit.

### Caution

Sensor outage breaks the link connecting the devices on either side of the Sensor for a brief moment and requires renegotiation of the network link between the two peer devices connected to the Sensor. Depending on the network equipment, this disruption introduced by the renegotiation of the link layer between the two peer devices might range from a couple of seconds to more than a minute with certain vendors' devices.

### Caution

A very brief link disruption might also occur when links between the Sensor and each of the peer devices are renegotiated to place the Sensor back in in-line mode. This outage, again, varies depending on the device, and can range from a few seconds to more than a minute. The performance of the switchover from in-line to bypass and vice versa varies depending on the vendor.

You can find the installation and troubleshooting instructions for the kit in the guide that accompanies the kit.

:

## Connect the cable for Sensor failover

For Sensor failover, connect two NS3x00 Sensors using the appropriate ethernet cables. These two Sensors must be running the same software version.

Refer to the following table before you configure a HA pair:

Sensor Model	Port to connect the HA pair	Cable requirements for failover
NS3100/NS3200	1	Ethernet copper cable (minimum Category 5e)

### Steps:

1. Plug the cable into port 1 of the active NS3x00 Sensor.

2. Connect the other end of the cable into port 1 of the standby NS3x00 Sensor. Only port 1 is required for failover to function properly.

:

## Turning the Sensor on and off

### Note

Do not attempt to turn on the Sensor until you have installed the Sensor in a rack and made all the necessary network connections.

#### Steps:

1. Connect the power cable to the Sensor power inlet.
2. Connect the power cable to a power source. The Sensor has no power switch. The Sensor turns on as soon as one of its power cables is connected to a power source. Trellix recommends that you use the **shutdown** CLI command to halt the Sensor before turning it off. For more information on CLI commands, see the *CLI commands* section in *Trellix Intrusion Prevention System Product Guide*.

:

## Configure the Sensor and Manager for deployment

:

### 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.

#### Steps:


1. Prepare the system according to the requirements outlined in *Trellix Intrusion Prevention System Installation Guide*.
2. Close all open applications.

3. Go to [Trellix Download Server](https://www.trellix.com/en-us/downloads/my-products.html) (<https://www.trellix.com/en-us/downloads/my-products.html>).
4. Log on using your **Grant Number** and registered **Email Address**.  
The Find Products page opens.
5. In the Category filter, select Network Security.
6. Click on the Manager version required.  
The Available Downloads page opens.
7. In the Type filter, select Installation.  
The Manager installation files available for download are listed.
8. Click on the required Manager installation file and the download starts.
9. Refer to *Trellix Intrusion Prevention System Installation Guide* for detailed procedure to install the Manager application.

:

## Add the Sensor to the Manager

### Steps:

1. Log on to the Manager using the default user name (**admin**) and password (**admin123**).
2. Go to Devices → <Admin Domain Name> → Global → Device Manager.  
The Device Manager page is displayed.
3. 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.

4. Enter the following mandatory information in the appropriate fields:

- Name — The Sensor name must begin with a letter. The maximum length of the name is 25 characters.
- 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 enter later 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.

- Device Type — Specifies the type of device to be added. Select IPS Sensor.
- Deployment Mode — Select Direct or Indirect.

#### Note

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

- Contact Information — (Optional) Type the contact information.
- Location — (Optional) Type the location.
- Comment — (Optional) Type the comment.

5. Click Save.

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

:

## 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.



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.

### Steps:

1. Log on to the Sensor using the terminal connected to the Console port.
2. At the prompt, log on using the default Sensor username (**admin**) and password (**admin123**).

```
login as: admin
* * *

Authorized users only. Unauthorized users will be prosecuted
to the full extent of the law.

* * *
Using keyboard-interactive authentication.
Password:
Last login: Fri Sep 28 07:20:31 2012 from 172.16.230.77
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is 'off'.

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

3. (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.

4. Set the name of the Sensor.



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.

At the prompt, type: **set sensor name <word>**. Example: **set sensor name HR\_sensor1**



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.

5. 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**
6. 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**
7. 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**



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.

8. If prompted, reboot the Sensor. Type **reboot**



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

9. 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 that the information is correct.
10. 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.

11. Type **show** to verify the configuration information. Check that all information is correct.
12. Type **exit** to exit the session.

:

**Verify successful installation****Steps:**

1. Type **status** in the Sensor CLI. The status report appears.

```

intruShell@> status
[Sensor]
System Initialized      : yes
System Health Status   : good
Layer 2 Status         : normal (IDS/IPS)
Installation Status    : complete
IPv6 Status            : Dont Parse and Allow Inline
Reboot Status         : Not Required
Guest Portal Status    : up
Hitless Reboot        : Available
Last Reboot reason    : reboot issued from CLI

[Signature Status]
Present                : yes
Version               :
Power up signature     : good
Geo Location database : Present
DAT file              : Present
DAT file Version      :

[Manager Communications]
Trust Established      : yes (Self Signed cert support)
Alert Channel         : up
Log Channel           : up
Authentication Channel : up
Last Error            : None
Alerts Sent           : 29254016
Logs Sent             : 27217316

[Alerts Detected]
Signature              : 29105690      Alerts Suppressed : 0
Scan                  : 12           Denial of Service : 132527
Malware                : 15807

[MATD Communication]
Status                : down
IP                    : 0.0.0.0
Port(Secure)         : 8505

```

The Sensor parameter **System Initialized** should be **yes**, and for Manager communication **Trust Established** should be **yes**.

2. Return to the Manager. In the Manager Home page, view the Manager status in the System Faults section. The Manager status should be up and Sensor status should be active.



System Faults				
Manager	Status	Critical	Error	Warning
Manager	Up	1	1	0
Device	Status	Critical	Error	Warning
_NS-series_Sensor_1	Active	6	0	3
_NS-series_Sensor_2	Active	4	1	3
NS9500_Stack-1	Unknown	0	0	0
NS9500_Stack-2	Unknown	0	0	0
_Sensor_1	Active	0	0	0
_Sensor_2	Active	1	0	0
_VM600_1	Active	0	0	0
_VM600_2	Active	0	0	0

- From the Manager Home page, click Configure to open the Configuration page.
- Select your added Sensor: Device List → <Device\_Name>. The ports for this Sensor appear under the <Device\_Name> node.

### Note

<Device\_Name> indicates the name of the Sensor you added.

Physical Ports					
Port	Link	Virtual Adapter	Operation Mode	Placement	Response Port
I/O Module: G0 (2-port Q5FP+ module detected)					
0/1	---	---	---	---	---
0/2	---	---	---	---	---
I/O Module: G1 (empty)					
---	---	---	---	---	---
I/O Module: G2 (empty)					
---	---	---	---	---	---
I/O Module: G3 (8-port RJ-45 module detected)					
3/1	⊘ Disabled		In-line Fail Open (Paired with 3/2)	Inside Network	This Port
3/2	⊘ Disabled		In-line Fail Open (Paired with 3/1)	Outside Network	This Port
3/3	✔ Up		In-line Fail Open (Paired with 3/4)	Inside Network	This Port
3/4	✔ Up		In-line Fail Open (Paired with 3/3)	Outside Network	This Port
3/5	✔ Up		In-line Fail Open (Paired with 3/6)	Inside Network	This Port
3/6	✔ Up		In-line Fail Open (Paired with 3/5)	Outside Network	This Port
3/7	⊘ Disabled		In-line Fail Open (Paired with 3/8)	Inside Network	This Port
3/8	⊘ Disabled		In-line Fail Open (Paired with 3/7)	Outside Network	This Port

- 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 IPS-provided policies, you can clone the policy and then customize it as described in *Trellix Intrusion Prevention System Product Guide*.

6. Click Device List → <Device\_Name> → Port Settings.
7. 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*.

:

## You're up and running!

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

### Steps:

1. For detailed usage instructions, see *Trellix Intrusion Prevention System Product Guide*, or click the ? buttons in the upper-right corner of each window in the Manager.
2. Start the Analysis → <Admin Domain> → Attack Log to view alert statistics as attacks are detected. A summary of alerts is displayed in the Unacknowledged Alert Summary monitor of the Manager Dashboard page.
3. Having problems? Check *Trellix Intrusion Prevention System Product Guide* for troubleshooting information.
4. 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://supportm.trellix.com>.

:

## Troubleshooting the Sensor

This section lists some common installation problems, the possible causes, and the corresponding solutions.

Problem	Possible Cause	Solution
LED is off	The Sensor is turned off.	Restore Sensor power.

Problem	Possible Cause	Solution
	The Sensor port cable is disconnected.	Check the Sensor cable connections.
Sensor is operational but not monitoring traffic	Network device cables have been disconnected.	Check the cables and make sure they are properly connected to both the network devices and the bypass switch.
	The Sensor ports have not been enabled in the Manager.	The Sensor will not monitor traffic on the ports unless the ports are enabled in the Manager. Ports are disabled in case of Sensor failure; you must re-enable them for Sensor monitoring to resume.
Network or link problems	Improper cabling or port configuration	Make sure that the transmitting and receiving cables are properly connected to the bypass switch.
Runts or giants errors on switch and routers	Improper cabling or port configuration	Make sure that the transmitting and receiving cables are properly connected to the bypass switch.
The critical fault, Switch absent appears in the Manager System faults page.	The fail-open kit is disconnected.	Check the fail-open kit and make sure it is properly connected to the Sensor.

For more information on troubleshooting steps and faults generated in the Manager, see the *Troubleshooting* section in *Trellix Intrusion Prevention System Product Guide*.

:

## Sensor technical specifications

The following table lists the specifications of an NS3x00 Sensor:

Sensor Specifics	NS3200	NS3100
Dimensions	1RU Rack Mountable 17.375" (W) x 1.75" (H) x 11.0" (D)	1RU Rack Mountable 17.375" (W) x 1.75" (H) x 11.0" (D)
Weight	8.1 lbs.	8.1 lbs.
Storage	Solid State 30 GB	Solid State 30 GB
<b>System Heat Dissipation</b>		
Maximum BTU	185	185
Typical BTU	104	104
Maximum Power Consumption	100W	100W
Power	100-240 VAC (50/60Hz)	
Temperature	Operating: 0°-35° C , Non-operating: - 40°- 70° C	
Relative humidity (non-condensing)	Operational: 10%-90%, Non-operational: 5%-95%	
Altitude	0 to 10,000 feet	
Safety Certification	UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB license and report covering all national country deviations.	
EMI Certification	FCC Part 15, Class A (CFR 47) (USA) ICES-003 Class A (Canada), EN55022 Class A (Europe), CISPR22 Class A (Int'l)	

:

## COPYRIGHT

Copyright © 2024 Musarubra US LLC.

Trellix and FireEye are the trademarks or registered trademarks of Musarubra US LLC, FireEye Security Holdings US LLC and their affiliates in the US and /or other countries. McAfee is the trademark or registered trademark of McAfee LLC or its subsidiaries in the US and /or other countries. Skyhigh Security is the trademark of Skyhigh Security LLC and its affiliates in the US and other countries. Other names and brands are the property of these companies or may be claimed as the property of others.

