



3.9.0

TippingPoint™

Intrusion Prevention System (IPS)

NX Series Stacking Deployment Guide

Actionable threat defense against known and zero-day attacks

Legal and notice information

© Copyright 2017 Trend Micro Incorporated. All rights reserved.

Trend Micro Incorporated makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Trend Micro Incorporated shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Trend Micro Incorporated. The information is provided “as is” without warranty of any kind and is subject to change without notice. The only warranties for Trend Micro Incorporated products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Trend Micro Incorporated shall not be liable for technical or editorial errors or omissions contained herein.

TippingPoint, the TippingPoint logo, and Digital Vaccine are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their respective owners. This document contains confidential information, trade secrets or both, which are the property of Trend Micro Incorporated. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from Trend Micro Incorporated or one of its subsidiaries.

All other company and product names may be trademarks of their respective holders.

TippingPoint Intrusion Prevention System (IPS) NX Series Stacking Deployment Guide
Publication Part Number: APEM37549/160824

Contents

- About this guide..... 1**
 - Related documentation..... 1
 - Product support..... 1
- Overview..... 2**
- Set up the stack..... 3**
 - Stacking components..... 3
 - Basic stack configuration..... 4
 - Install the stacking components..... 4
 - Create the stack in the SMS..... 5
 - Add the stacking devices to the SMS..... 6
 - Create the stack..... 6
 - Distribute the inspection profile..... 8
 - Resilient stack configuration..... 9
 - Multiple network segment device configuration..... 10
- Update the stack configuration..... 12**
 - Enable or disable stack resiliency..... 12
 - Change the segment reference device..... 13
 - Replace a device in the stack..... 13
 - Remove a device from the stack..... 14
 - Add a device to the stack..... 15
 - Delete the stack..... 16
 - Rename segments..... 16
 - Grant permissions to the stack..... 17

Add stack management to the user role.....	17
Grant the user group access to the stack.....	17
Distribute a TOS update.....	18
Troubleshooting.....	19
Verify AOC cable installation.....	19
View stacking status.....	21
Device details.....	21
Front panel stacking LEDs.....	23
Device shelf-level graphic.....	24
Verify stack health and synchronization.....	25
View overall health of the stack.....	25
Verify stacking bus state.....	28
Verify stack member state.....	31
Verify device state.....	32
Verify stack synchronization.....	33
Resolve issues adding a device to the stack.....	40
View stacking tier statistics.....	42
Enable or disable Intrinsic High Availability Layer-2 Fallback.....	43
Enable or disable Intrinsic HA L2FB on the stack.....	44
Enable or disable Intrinsic HA L2FB on a stacking device.....	44
Export a Tech Support Report from an IPS device.....	45
CLI commands for stacking.....	46
show stacking.....	46
Limitations.....	49
Repurpose a device.....	50
Stacking terminology.....	51

AOC cable.....	51
Intrinsic HA.....	51
network segment.....	51
network segment device.....	51
Not Ready to Inspect (NRTI).....	51
Ready to Inspect (RTI).....	51
segment reference device.....	52
stack master.....	52
stack resiliency.....	52
stacking.....	52
stacking bus.....	52
stacking port.....	52

About this guide

This guide is intended for network administrators and specialists who monitor and manage system security. The information provided describes how to increase inspection capacity by implementing stacking for TippingPoint NX Series Intrusion Prevention System (IPS) devices.

This section covers the following topics:

- [Related documentation](#) on page 1
- [Product support](#) on page 1

Related documentation

A complete set of documentation for your product is available on the TippingPoint Threat Management Center (TMC) at <https://tmc.tippingpoint.com>. The documentation generally includes installation and user guides, command line interface (CLI) references, safety and compliance information, and release notes.

Product support

Information for you to contact product support is available on the TMC at <https://tmc.tippingpoint.com>.

Overview

Stacking enables you to increase the overall inspection capacity of your TippingPoint Intrusion Prevention System (IPS) by grouping multiple NX Series devices and pooling their resources.

You can configure up to five NX Series devices in a stack. The stack operates as a single device that you manage on the TippingPoint Security Management System (SMS). All devices in the stack must be the same model, either 7100NX or 7500NX.

In-line inspection capacity increases with each device that you add to the stack. For example, for each 7500NX added to a stack of 7500NX devices, the inspection capacity increases by 20 Gbps.

The following TippingPoint software is supported for stacking:

- **TippingPoint SMS v4.5.0, or later** - Centrally manages each stack of devices.
- **TippingPoint Operating System (TOS) v3.9.0, or later** - Must be installed on each security device.

Note: No additional licensing is required to implement stacking.

Not all TippingPoint NX Series IPS features are supported in a stack configuration. See [Limitations](#) on page 49.

Set up the stack

This information explains how to set up the stack of devices, including basic, resilient, and multiple network segment configurations.

You can customize the stack by adding the number of devices and enabling the features you need.

After you set up a basic stack, you can consider whether to configure it to be a resilient stack. For more information, see [Resilient stack configuration](#) on page 9.

For details about how to install your security device, see the *Install your security device* quick reference card.

Stacking components

You need the following components for each device that you add to the stack. Also, you need network I/O modules for the stack members that you connect to the network.

- TippingPoint 7100NX or 7500NX device (each member of the stack must be the same model).



- The 40 GbE QSFP+ I/O module (installed in slot 4).



- TippingPoint 40G QSFP+ Active Optical Cable (AOC).



Basic stack configuration

When you configure a basic stack, every member of the stack must be operational. If any member of a basic stack becomes unavailable, the entire stack becomes unavailable. Use the following information to configure a basic stack:

- [Install the stacking components](#) on page 4
- [Create the stack in the SMS](#) on page 5

Install the stacking components

An NX Series device stack requires the 40 GbE QSFP+ I/O module to always be installed in slot 4 of each device. You can use slots 1–3 for network I/O modules.

The I/O modules should be installed in the stacking device that you plan to use as the network segment device. A *network segment device* operates in-line in the network and distributes network traffic to each stack member for inspection. The other stack members do not need network I/O modules.

When you connect the AOC cables, use a ring topology so that each device connects to its peer.

To install the stacking components

1. Install the network I/O modules on the network segment device in **slots 1–3** so that you can connect the device to the network.
2. Install the 40 GbE QSFP+ I/O module in slot 4 of both devices so that you can connect the devices to the stacking bus.

The *stacking bus* consists of a 40 GbE QSFP+ I/O module on each stacking device that connects the stack in a ring topology.

For more information about how to install I/O modules, see the *NX-Platform Hardware Installation and Safety Guide*.

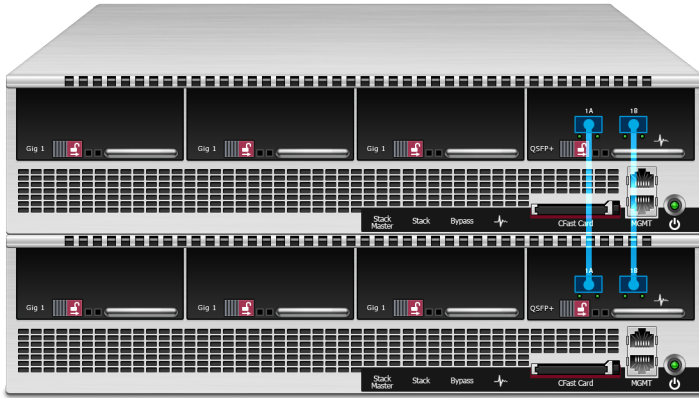
3. Install the AOC cables in slot 4 of both devices so that each device connects to its peer in a ring topology.

Note: When you install the AOC cable, you should orient the QSFP+ transceiver with the tab **on top**. The AOC cable is keyed so that it can only be correctly inserted one way. If the cable does not slide in easily and click to latch, it may be upside down. See [Verify AOC cable installation](#) on page 19 for more information.

Examples with the 40 GbE QSFP+ I/O modules and the AOC cables installed

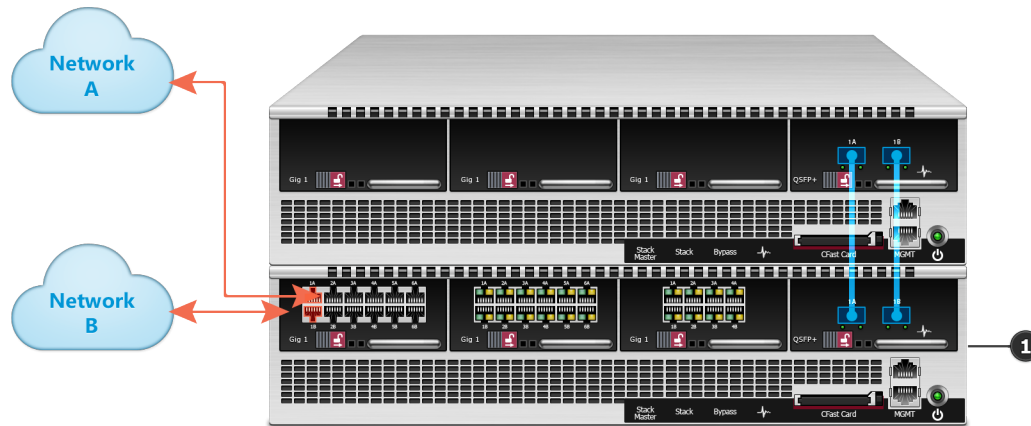
The following example shows the 40 GbE QSFP+ I/O modules are installed in slot 4 and the AOC cables are installed.

Figure 1. TippingPoint NX Series IPS – 40 GbE QSFP+ I/O modules are installed in slot 4 and the AOC cables are installed properly



The next example shows the network I/O modules are installed in slots 1, 2, and 3 of the network segment device (1).

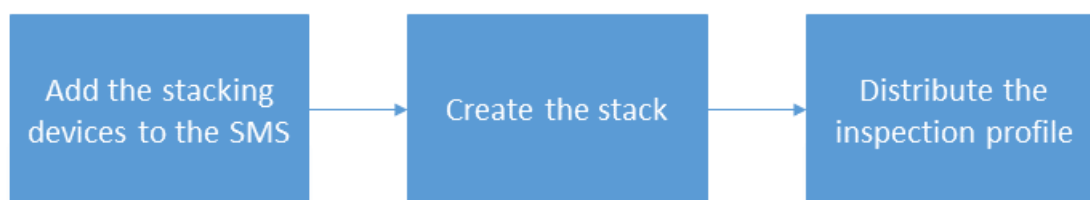
Figure 2. TippingPoint NX Series IPS – stack with network I/O modules installed in slots 1–3



Create the stack in the SMS

Use the SMS to create the stack and centrally manage the stacking devices online.

The process is:



The following information provides more details:

- [Add the stacking devices to the SMS](#) on page 6
- [Create the stack](#) on page 6
- [Distribute the inspection profile](#) on page 8

Note: Before you can create the stack in the SMS, you need to set up the stacking components. See [Install the stacking components](#) on page 4.

Add the stacking devices to the SMS

After you install the stacking components, add each device in the stack to the SMS so that you can create and manage the stack online.

For each device, use the SMS to install the required TippingPoint Operating System (TOS) version, v3.9.0 or later. The TOS version must be the same on each NX Series device. For more information, see the *Security Management System User Guide*.

If you are repurposing an existing device for use in the stack, reset the device to factory settings, and then install the required TOS version. For more information, see [Repurpose a device](#) on page 50.

Create the stack

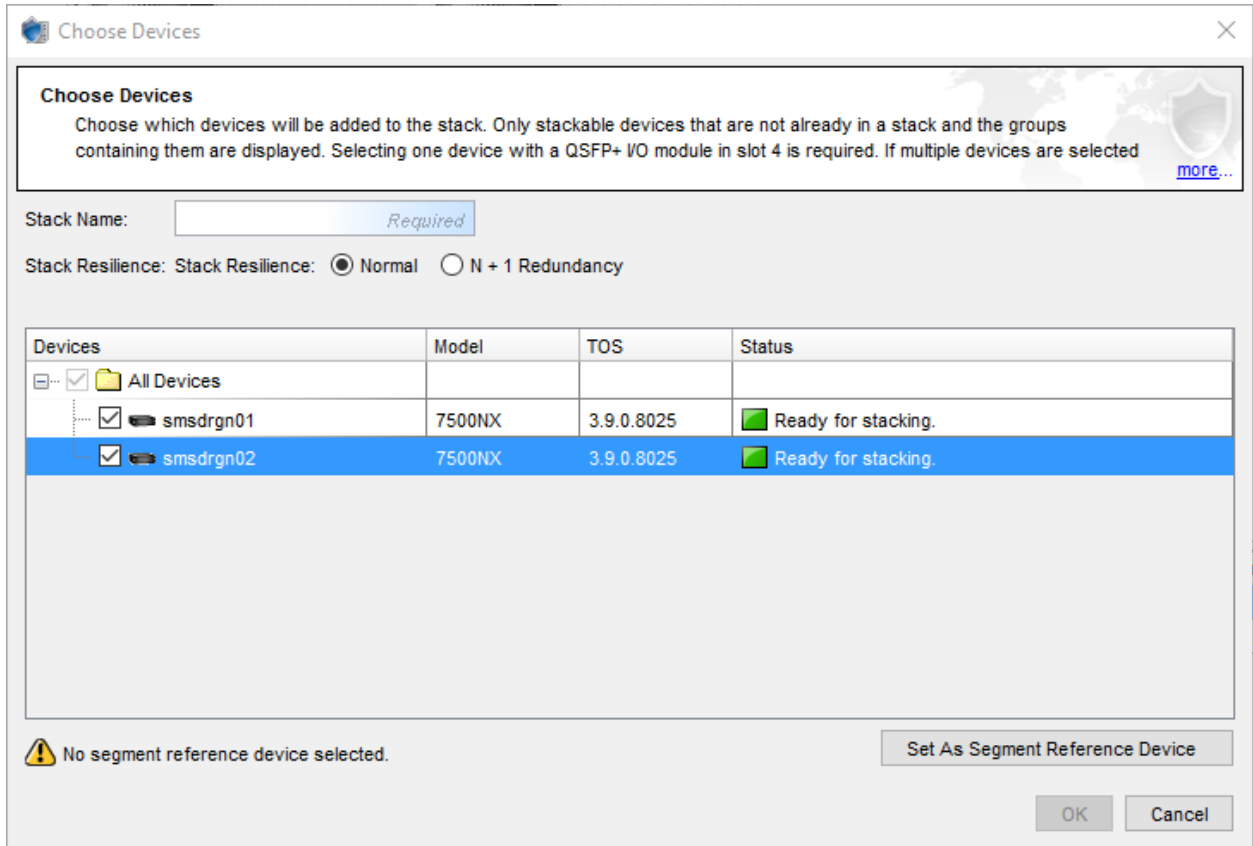
After you add the stacking devices to the SMS, create the stack in the SMS so that the devices are in the stacking topology. Then, use the Devices options in the SMS to specify the stack configuration.

Note: You must have a SuperUser role for SMS administration to create a stack. For more information, see the *Security Management System User Guide*.

To create the basic stack in the SMS with two devices

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, right-click a stacking device and select **New Stack**.
3. In the **Choose Devices** options, specify the stack name.

Figure 3. Choose devices options – stacking devices selected



4. Choose **Normal** for the Stack Resilience option.

For information about the **N+1 Redundancy** option, see [Resilient stack configuration](#) on page 9.

5. Select both devices.
 - If a device is not displayed, validate the following items:
 - The device is not already a member of another stack.
 - The device is the same model as the other selected devices.
 - If either device does not have a **Ready for stacking** status, see [Resolve issues adding a device to the stack](#) on page 40 for troubleshooting information.
6. Click **Set as Segment Reference Device** and select the network segment device that the SMS uses as a template to create the corresponding segments on each stack member.
7. Click **OK**.
8. In the **All Devices** workspace, double-click the stack shelf-level image to view stack health.
9. In the **Summary** tab, verify the stack health is Normal.

If the stack is not healthy, identify and resolve any issues. See [Verify stack health and synchronization](#) on page 25.

Distribute the inspection profile

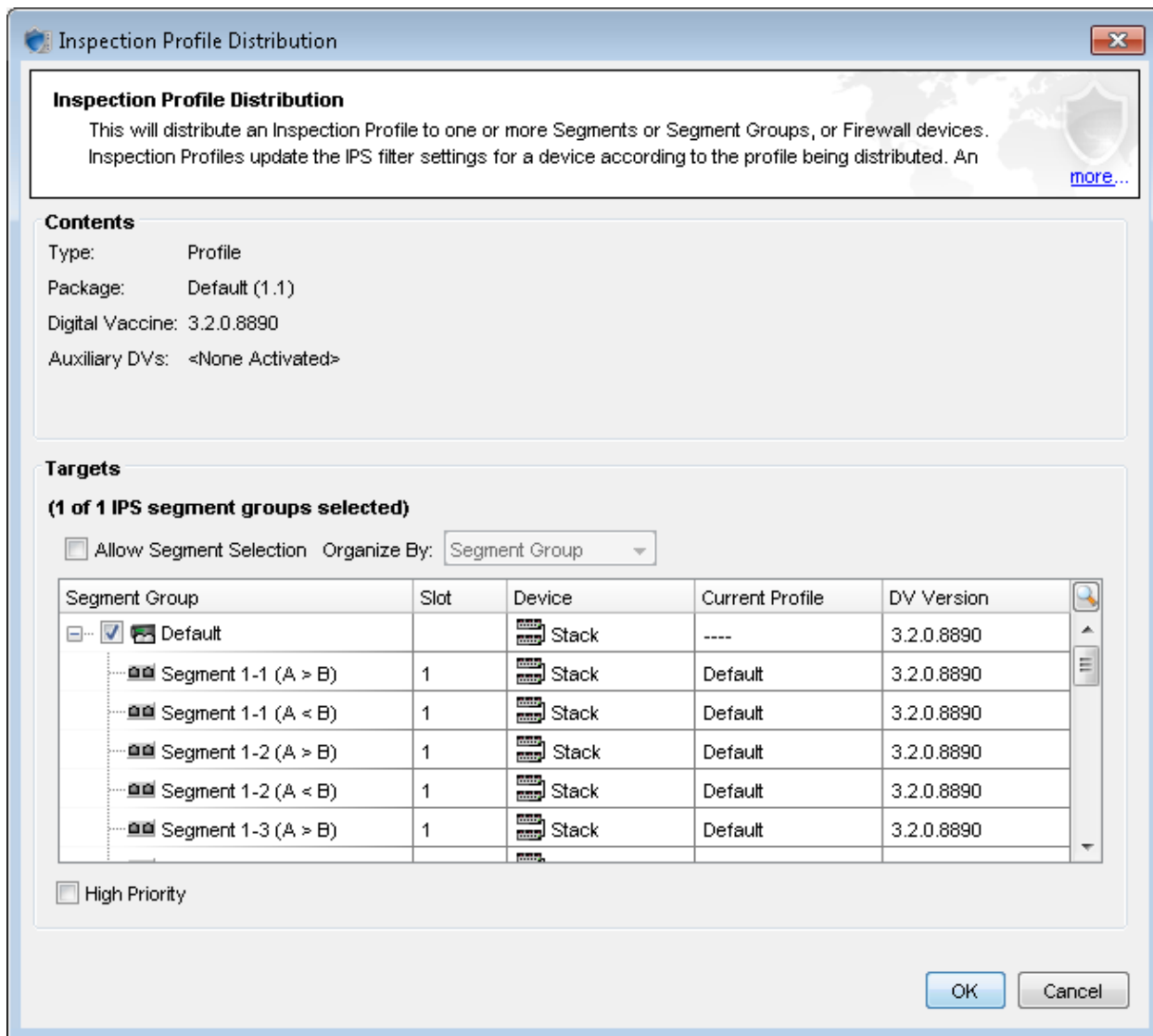
Distribute the inspection profile to the stack by choosing from the segments on the segment reference device (SRD). After you do this, the inspection profile goes to the corresponding segments on each member of the stack.

Note: For more information, see the *Security Management System User Guide*.

After you distribute the inspection profile, use the **Sync Health** tab to identify and resolve any synchronization issues with the stack. See [Verify stack synchronization](#) on page 33.

The following example shows the profile distribution to the default segment group, which includes all the segments on the stack.

Figure 4. Distribute the inspection profile to all the segments on the stack



Resilient stack configuration

You can change the configuration of a basic stack to a resilient stack so that the stack continues to inspect network traffic if a single stack member is not ready to inspect (NRTI).

In a *resilient stack*, the network traffic continues to be inspected when a single stack member is NRTI by rebalancing network traffic between the remaining ready to inspect (RTI) devices. For information about how stacking determines whether a device is ready to inspect, see [Enable or disable Intrinsic High Availability Layer-2 Fallback](#) on page 43.

To enable a resilient stack configuration, follow the same process that is described in [Create the stack](#) on page 6, but select the **N+1 Redundancy** Stack Resiliency option.

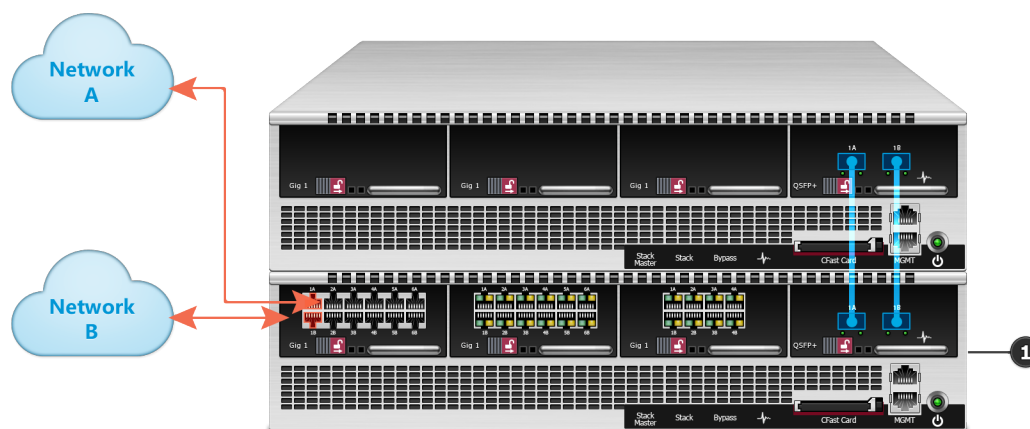
When all the devices in the stack are RTI, the stack load balances network traffic across all the devices. If a single stack member is NRTI, the stack rebalances network traffic between the remaining RTI devices, reducing inspection capacity.

Important: When the stack is configured with a single network segment device, if the network segment device is NRTI, the entire stack is NRTI. To enable the stack to continue to inspect traffic when the network segment device is NRTI, configure multiple network segment devices. See [Multiple network segment device configuration](#) on page 10.

The following example shows a resilient stack:

- The network segment device (1) is at the bottom of the stack.
- The network segment device load-balances network traffic from each utilized segment to the other device in the stack.
- The stack continues to inspect if the top device is unavailable.

Figure 5. TippingPoint NX Series IPS – resilient stack configuration



Multiple network segment device configuration

You can change the device configuration of a resilient stack to include multiple network segment devices. With more than one network segment device, the stack continues to inspect network traffic if any stack member, *including a network segment device*, becomes unavailable. If any stack member becomes unavailable, the stack rebalances network traffic between the remaining available devices.

To configure multiple network segment devices

- Install network I/O modules on each network segment device.

The same slot on each device must be configured with either the **same** network I/O module or **no** network I/O module.

Consider the following items when you configure multiple network segment devices:

- Connect the same networks to the same network segments on each network segment device.
- Traffic can come in both network segment devices as long as the corresponding segment ports of each device are connected to the same networks. For example, port 1–1A on IPS–A and IPS–B are connected to Network A and port 1–1B on IPS–A and IPS–B are connected to Network B.

Example with multiple network segment devices

The following example shows a valid two-device stack with both network segment devices connected to the same networks on the same segment ports. Either network segment device can be designated as the segment reference device. Each network segment device load-balances traffic from each utilized segment to the other member of the stack on a per flow basis.

Figure 6. TippingPoint NX Series IPS – two-device stack with multiple network segment devices



Update the stack configuration

In the SMS, update the stack configuration, for example, when you need to add another device to the stack.

Note: For information about the differences between configuring a stack of devices compared with configuring a standalone device, see the *Security Management System User Guide*.

The following information describes several ways that you can update the stack configuration:

- [Enable or disable stack resiliency](#) on page 12
- [Change the segment reference device](#) on page 13
- [Replace a device in the stack](#) on page 13
- [Remove a device from the stack](#) on page 14
- [Add a device to the stack](#) on page 15
- [Delete the stack](#) on page 16
- [Rename segments](#) on page 16
- [Grant permissions to the stack](#) on page 17
- [Distribute a TOS update](#) on page 18

Enable or disable stack resiliency

Update the stack configuration in the SMS to enable stack resiliency so that the stack can continue to inspect traffic if a single stack member is not ready to inspect (NRTI) network traffic.

When you enable stack resiliency, make sure the stack is configured with enough devices to provide the required inspection capacity. See [Resilient stack configuration](#) on page 9.

To enable or disable stack resiliency

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. In the **Summary** tab, click **Edit**.
4. In **Edit Stack Configuration**, select a Stack Resilience option:
 - **N+1 Redundancy** – This option enables the stack to continue to inspect traffic if a single stack member is NRTI. If more than one device is NRTI, the stack automatically goes into Intrinsic HA L2FB. See also, [Enable or disable Intrinsic High Availability Layer-2 Fallback](#) on page 43.

- **Normal** – This option automatically places the stack into Intrinsic HA L2FB if a single stack member is NRTI.

Change the segment reference device

Update the stack configuration in the SMS to select the network segment device that the SMS uses as a template to create the corresponding segments on each stack member.

Make sure that the device is configured with the correct network I/O modules, has the correct segment configuration, and has the associated inspection policy.

After you change the segment reference device, distribute the inspection profile to update the stack. For more information, see [Distribute the inspection profile](#) on page 8.

To change the segment reference device in the SMS

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. In the **Summary** tab, click **Edit**.
4. In **Edit Stack Configuration** options, select the network segment device from the Segment Reference Device list.

Replace a device in the stack

If a stacking device must be replaced, you can update the stack configuration in the SMS with the replacement device.

If any of the physical segments on the stacking device were renamed, rename the segments on the replacement device. For more information, see [Rename segments](#) on page 16.

To replace a stack member in the SMS

1. Place the stack in Intrinsic HA L2FB. See [Enable or disable Intrinsic HA L2FB on the stack](#) on page 44.
2. Remove the stack member from the stack configuration. See [Remove a device from the stack](#) on page 14.

If the device is designated as the segment reference device (SRD), update the stack configuration to designate a different device as the SRD, and then remove the stack member from the stack configuration. See [Change the segment reference device](#) on page 13.

3. Install the AOC cables to remove the old stacking device from the stacking bus and to add the new device. See [Install the stacking components](#) on page 4.

If the device you want to replace is configured with network I/O modules, make sure that the replacement device has the same network I/O modules in the same slots.

4. Manage the new device with the SMS and then add the stacking device to the stack configuration. See [Add a device to the stack](#) on page 15.

If necessary, update the stack configuration to designate the replacement device as the SRD. See [Change the segment reference device](#) on page 13.

5. Distribute the inspection profile to the stack. For more information, see [Distribute the inspection profile](#) on page 8.
6. Take the stack out of Intrinsic HA L2FB. See [Enable or disable Intrinsic HA L2FB on the stack](#) on page 44.

Remove a device from the stack

Remove a device from the stack when you need to decrease inspection capacity, or when you need to replace a device in the stack.

(Best Practice) To reuse a device after it is removed from the stack, either as a standalone device or as part of a different stack, use the `debug factory-reset` command to restore the device to its original settings. See [Repurpose a device](#) on page 50.

Note: A stack with a single stack member is supported on a temporary basis, for example, to replace a device in the stack with two devices. However, a single-device stack does not have a normal health status.

To remove a device from the stack configuration

1. Place the stack in Intrinsic HA L2FB. See [Enable or disable Intrinsic HA L2FB on the stack](#) on page 44.
2. Remove the device from the stack in the SMS (see the next procedure).

If the device is designated as the segment reference device (SRD), update the stack configuration to designate a different device as the SRD, then remove the device from the stack configuration. See [Change the segment reference device](#) on page 13.

3. Install the AOC cables to remove the old stacking device from the stacking bus. See [Install the stacking components](#) on page 4.
4. Take the stack out of Intrinsic HA L2FB. See [Enable or disable Intrinsic HA L2FB on the stack](#) on page 44.

To remove a device from the stack in the SMS

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. In the **Summary** tab, select a device from the Stack Member list.
4. Click **Remove**.
5. Click **OK**.

The stack health is updated. See [Verify stack health and synchronization](#) on page 25.

Add a device to the stack

Add a device to the stack when you need to increase the inspection capacity of the stack, or when you need to replace a device in the stack.

(Best Practice) If you are repurposing an existing device for use in the stack, reset the device to factory settings, and then install the required TOS version. See [Repurpose a device](#) on page 50.

When you add a device to the stack configuration, the SMS automatically enables stacking on the device. If necessary, remove the device from the stack configuration, and then add it again to enable stacking. See [View overall health of the stack](#) on page 25.

If any of the physical segments on the stack were renamed, if necessary, rename the segments on the new device. For more information, see [Rename segments](#) on page 16.

To add a device to the stack configuration

1. Place the stack in Intrinsic HA L2FB. See [Enable or disable Intrinsic HA L2FB on the stack](#) on page 44.
2. Install the AOC cables to add the device to the stacking bus. See [Install the stacking components](#) on page 4.
3. Add the stacking device to the SMS. See [Add the stacking devices to the SMS](#) on page 6.
4. Add the device to the stack in the SMS (see the next procedure).
5. Distribute the inspection profile to the stack. For more information, see [Distribute the inspection profile](#) on page 8.
6. Take the stack out of Intrinsic HA L2FB. See [Enable or disable Intrinsic HA L2FB on the stack](#) on page 44.

After you add a device to the stack, update any scheduled profile distributions to include the new stack member as a target for the distribution.

Note: For information about where the options are different for managing a stack of devices instead of a single device, see the *Security Management System User Guide*.

Note: You must have permission to manage a device in order to add the device to a stack. See [Grant permissions to the stack](#) on page 17.

To add a device to the stack in the SMS

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. In the **Summary** tab, click **Add**.
4. Select the device to add.

If the device cannot be added to the stack, identify and resolve the issue. For troubleshooting information, see [Create the stack](#) on page 6.

5. Click **OK**.

The stack health is updated. See [Verify stack health and synchronization](#) on page 25.

6. If the device you are adding is intended to be the segment reference device (SRD), update the stack configuration to designate the device as the SRD. See [Change the segment reference device](#) on page 13.
7. Distribute the inspection profile

Delete the stack

Delete the stack to return the devices to the SMS as standalone devices.

After you delete the stack:

- The devices continue to be managed by the SMS.
- Stacking is **disabled** on each device.
- The inspection policies on all stacking devices are preserved.
- Any scheduled profile distributions continue to run on all the devices that were in the stack.

Note: For information about the differences between configuring a stack of devices compared with configuring a standalone device, see the *Security Management System User Guide*.

To delete the stack

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, right-click the stack and click **Delete Stack**.

The stack is removed and its devices are displayed in All Devices.

Rename segments

On slots 1–3, you can rename a physical segment and optionally, propagate that segment name to the corresponding segment on each member of the stack. Slot 4 is reserved for the stacking bus.

(Best Practice) Do not modify segment details other than the segment name. Across the stack, each segment must have the same configuration.

Tip: Use the **Rename across stacked device segments** option to propagate physical segment names across the stack, including any segment that does not have a network I/O module installed.

If you add or replace a stack member, if necessary, update any segment names on the new device. For example, if the new device does not have a network I/O module installed, use the **Rename across stacked device segments** option to propagate physical segment names across the updated stack configuration.

For more information, see the *Security Management System User Guide*.

Grant permissions to the stack

In the SMS, grant permissions to the stack so that an assigned user group can perform the following functions:

- Create, update, or delete the stack
- Add a device to or remove a device from the stack

The following information describes how to grant permissions to the stack:

- [Add stack management to the user role](#) on page 17
- [Grant the user group access to the stack](#) on page 17

Add stack management to the user role

In the SMS, grant permission to a user role to manage a stack.

This capability requires the user group to also have access to the stack. See [Grant the user group access to the stack](#) on page 17.

To update the user role

1. In the SMS tools, click **Admin**.
2. In the left navigation pane, expand **Authentication and Authorization > Roles**.
3. In the **User Roles** workspace, select the user role and click **Edit**.
4. In **Capabilities** options, click **Devices**.
5. Select the **Device Group/Stack Management** capability.

Grant the user group access to the stack

In the SMS, grant the user group access to the stack. With access to the stack, and permission to manage the stack, the user group can perform basic operations on the stack.

To grant the user group access to the stack

1. In the SMS tools, click **Admin**.
2. In the left navigation pane, expand **Authentication and Authorization > Groups**.
3. In the **User Groups** workspace, select the user group you want and click **Edit**.

4. In **Devices** options, select each stack you want from the list of devices.

Distribute a TOS update

Distribute a TOS update to the stack so that each stack member is updated with the same TOS version.

(Best Practice) Before you distribute a TOS update, enable Intrinsic HA L2FB on the stack. Installing a new software package forces a reboot of each stacking device, but Intrinsic HA L2FB remains enabled until the stack master confirms that there are enough devices in the stack that are ready to inspect (RTI). For more information, see [Enable or disable Intrinsic HA L2FB on the stack](#) on page 44.

Distribute a TOS update to the stack using the same steps you would follow for a standalone TippingPoint NX Series IPS. For more information, see the *Security Management System User Guide*.

Use the **Sync Health** tab to verify that the same TOS version is installed on each stacking device. For more information, see [Verify stack synchronization](#) on page 33.

Note: If the TOS update does not install properly on a stack member, distribute the TOS update to the stack again. If the stacking device has issues, remove it from the stack to make any updates, and then add the device to the stack. For more information, see [Remove a device from the stack](#) on page 14.

Troubleshooting

Use the following information to identify and resolve stacking issues:

- *Verify AOC cable installation* on page 19
- *View stacking status* on page 21
- *Verify stack health and synchronization* on page 25
- *Resolve issues adding a device to the stack* on page 40
- *View stacking tier statistics* on page 42
- *Enable or disable Intrinsic High Availability Layer-2 Fallback* on page 43
- *Export a Tech Support Report from an IPS device* on page 45
- *CLI commands for stacking* on page 46

For general troubleshooting information and system log messages, see:

- *Security Management System User Guide*
- *IPS System Log Messages Reference*

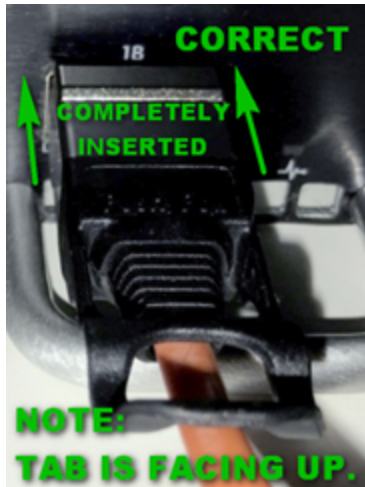
Verify AOC cable installation

The following information describes how to verify the AOC cable installation. Also, you can use this information to verify the installation of a QSFP+ transceiver.

Examples of a stacking port with the AOC cable installed

The following example shows a stacking port with the AOC cable installed correctly.

Figure 7. TippingPoint NX Series IPS – stacking port with the AOC cable installed correctly



The next example shows a stacking port with the AOC cable installed incorrectly.

Figure 8. TippingPoint NX Series IPS – stacking port with the AOC cable installed incorrectly



View stacking status

In the SMS, use the **Devices** workspace to view and manage the stack and its devices.

See the *Security Management System User Guide* for more information.

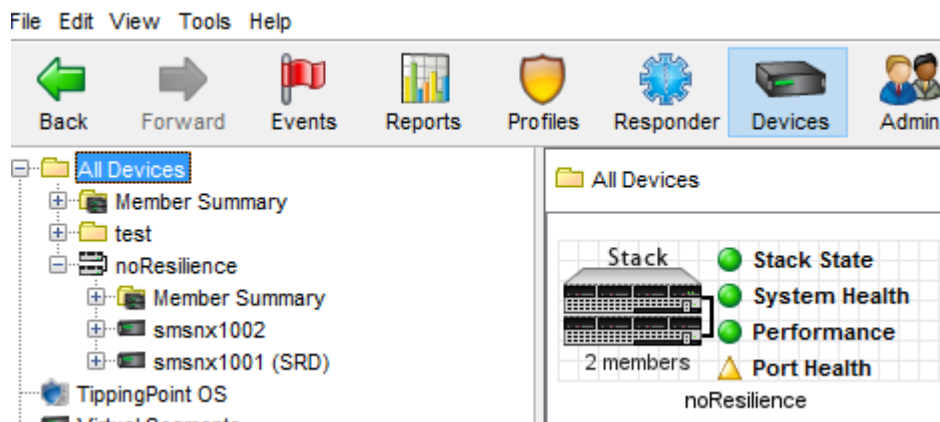
Device details

In the SMS, the **All Devices** workspace provides a consolidated view of information and configuration settings for the stack and individual stack members. Click **Stack State** to view stacking details and verify stack health.

The following information describes the device detail states for a stack.

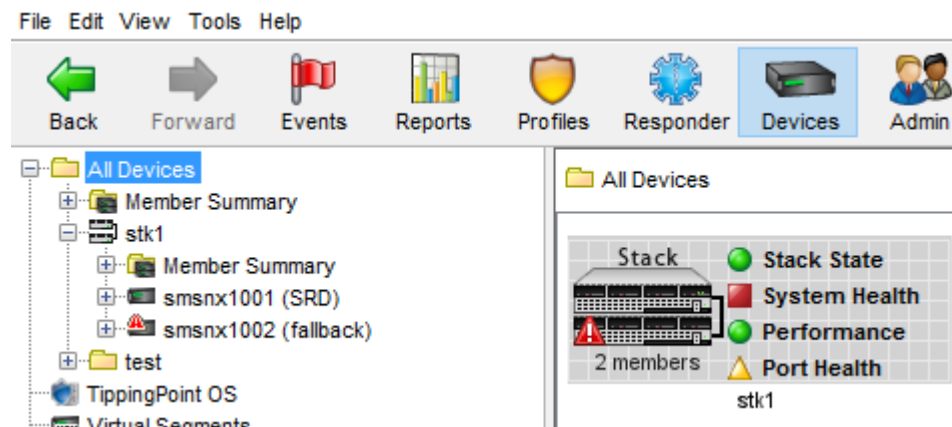
Stack is normal

The stack state is normal.




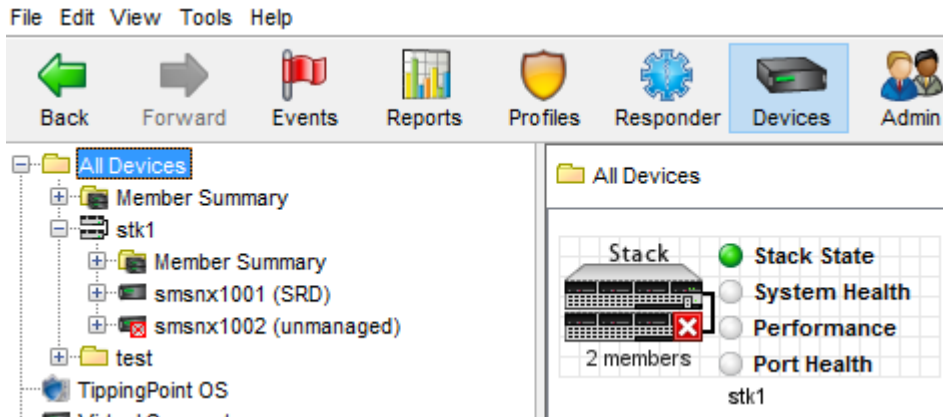
Stack with a device in Intrinsic HA L2FB

The  icon indicates that a device is in Intrinsic HA L2FB.





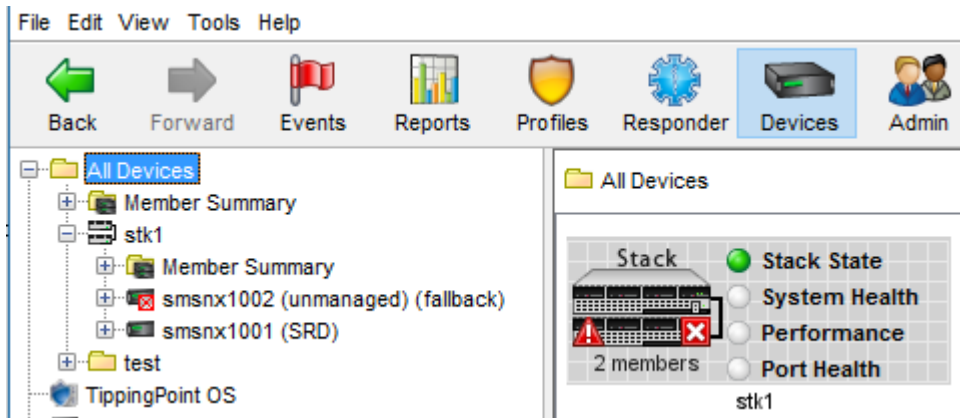
Stack with an unmanaged device

The  icon indicates that the **smsnx1002** device is unmanaged by the SMS and another device could be in Intrinsic HA L2FB. The navigation pane indicates that the **smsnx1001** device is the segment reference device (SRD) for the stack.




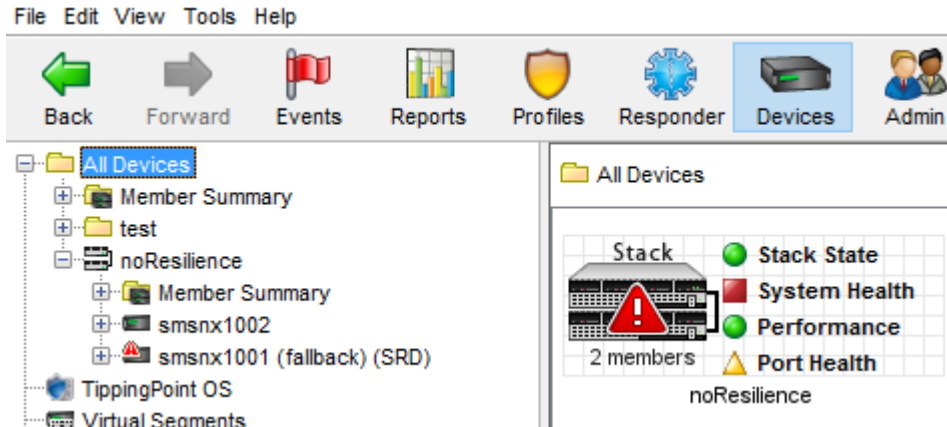
Stack with an unmanaged device that is also in Intrinsic HA L2FB

The  icon and the  icon indicate that a device is not managed by the SMS and another can be in Intrinsic HA L2FB.



Stack is in Intrinsic HA L2FB

The  icon indicates the stack is in Intrinsic HA L2FB.



Front panel stacking LEDs

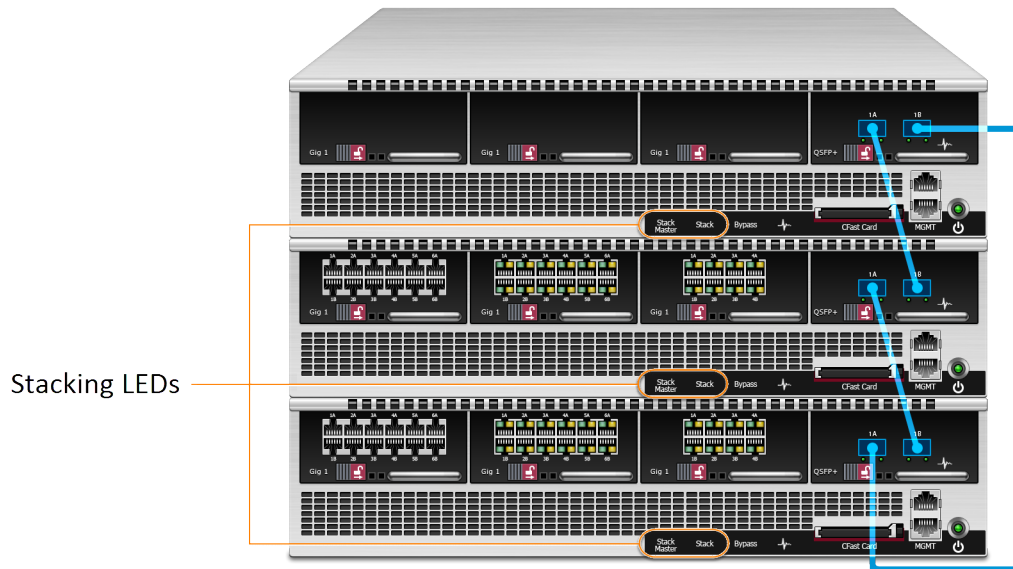
Use the front panel stacking LEDs to identify the stacking status on the device:

- **Stack:** When lit, indicates that stacking is enabled on the device. Stacking is automatically enabled when you use the SMS to add the device to the stack. If necessary, remove the device from the stack and then add it again to enable stacking. LED color indicates the following states:
 - **Flashing green:** Indicates that the device is ready to inspect (RTI) and is waiting for the stack master to allow the device to begin inspecting network traffic.
 - **Solid amber:** Indicates that the device is not ready to inspect (NRTI).
 - **Solid green:** Indicates that the device is RTI and inspecting network traffic. This is the normal operating mode.
- **Stack Master:** When lit (solid green), indicates that the device is the stack master.

The *stack master* is a device role that is responsible for managing stack configuration and states. The stack master is automatically elected by the devices in the stack. All stack members are eligible for election to stack master.

The following example shows the stacking LEDs on the front of each device in the stack:

Figure 9. TippingPoint NX Series IPS – stacking LEDs on front panel

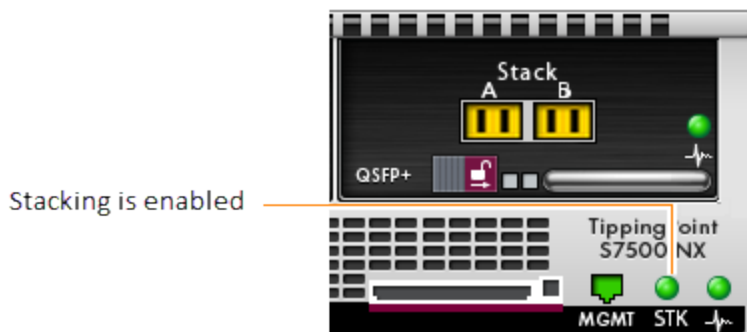


Device shelf-level graphic

In the SMS, use the device shelf-level graphic to identify the stacking status on the device:

- **STK** LED indicates whether stacking is enabled. In the following example, the **STK** LED is green to indicate stacking is enabled.
- In slot 4, the 40 GbE QSF+ I/O module is installed.
- The Stack **A** and **B** ports indicate whether the AOC cables are installed. The following example shows the stacking ports are yellow to indicate the AOC cables are not installed.

Figure 10. TippingPoint NX Series IPS – shelf-level graphic with open stacking ports



Verify stack health and synchronization

Use the SMS to identify and resolve stack health and synchronization issues. In the **All Devices** workspace, double-click the stack to view its status information:

- Use the **Summary** tab to verify the health of the stack. The icon on the **Summary** tab indicates the most severe status for the stack. If the stack is in a degraded state, use the Stack Members table to troubleshoot and resolve any issues.

(Best Practice) Perform stack health troubleshooting steps in the following order:

- a. *View overall health of the stack* on page 25
 - b. *Verify stacking bus state* on page 28
 - c. *Verify stack member state* on page 31
 - d. *Verify device state* on page 32
- Use the **Sync Health** tab to verify the synchronization status of each device in the stack. The icon on the **Sync Health** tab indicates the most severe synchronization status for the stack. If synchronization is in a degraded state, use the Issues table to troubleshoot and resolve any issues. For more information, see *Verify stack synchronization* on page 33.

View overall health of the stack

The **Summary** tab displays the current stack configuration, overall stack state, and the status of the stacking bus topology. If the status of the stack is not green (normal), identify and resolve any issues.







To view overall health of the stack





1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. In the **Summary** tab, use the stack health summary information to identify the current health of the stack and its configuration.
 - **Stack name** — Indicates the name of the stack. Click **Edit** to rename the stack.
 - **Stack state** — Indicates the current state of the stack as reported by the segment reference device.

Note: If the Stacking State is not normal, use the **Stack Port A** and **Stack Port B** columns, along with the **Status** column, to troubleshoot and resolve any issues.

The following information provides stacking port status information and suggested actions.

Table 1. Stacking port status



Status	Information	Suggested action
 Ready to Inspect - Normal	Indicates that the stack is working correctly.	No action is required.
 Not Ready to Inspect - Unknown	Indicates that the stack is not inspecting traffic for an unknown reason.	This is a transitory state and no action is required.
 Not Ready to Inspect - Rebooting	Indicates that the stack is not inspecting traffic because one or more of the stack members is rebooting.	This is a transitory state and no action is required.
 Not Ready to Inspect - Layer 2 Fallback	Indicates that the stack is not inspecting traffic because one or more of the devices is stuck in Intrinsic HA L2FB.	At a minimum, reboot the device. If the device returns to this state, a hardware-related issue is likely.
 Not Ready to Inspect - Recoverable Layer 2 Fallback	Indicates that the stack is not inspecting traffic because one or more of the devices is waiting for you to disable Intrinsic HA L2FB.	Disable Intrinsic HA L2FB on the stack. See Enable or disable Intrinsic HA L2FB on the stack on page 44.
 Not Ready to Inspect - Invalid	Indicates that the stack is not inspecting traffic because one or more devices has not completed the boot sequence.	Validate that each device has completed its boot sequence. To validate a particular device, log in to its serial interface and look for Run Level 12 in the boot sequence. If necessary, reboot the device.

Status	Information	Suggested action
	Indicates that the number of devices in the stack does not match the SMS stack configuration.	Validate that the number of devices that are cabled together in the stacking bus correspond to the stack configuration in the SMS.
 Ready to Inspect - Layer 2 Fallback	Indicates that the stack is in Intrinsic HA L2FB but can return to  Ready to Inspect - Normal when the stack master determines that the minimum number of devices are ready to inspect.	Depending on whether you configured the stack for resiliency, all but one of the stack members, or all of the stack members must declare they are  Ready to Inspect - Normal before the stack master returns the stack to  Ready to Inspect - Normal. See Enable or disable stack resiliency on page 12.

- **Stacking bus** — Indicates the current state of the stacking bus topology.

The following information provides stacking bus status information and suggested actions.

Table 2. Stacking bus topology state

Status	Information	Suggested Action
 Connected in a ring	Indicates that the AOC cables are installed correctly.	No action is required.
 Not Connected in a ring	Indicates that the AOC cables are not installed correctly.	Verify the stacking bus health. See Verify stacking bus state on page 28. See also, Install the stacking components on page 4.

- **Stack Resilience** — Indicates whether the stack goes into Intrinsic HA L2FB if a single device is not ready to inspect (NRTI). See [Enable or disable Intrinsic High Availability Layer-2 Fallback](#) on page 43.

- **Segment Reference Device** — Indicates the network segment device that the SMS uses as a reference to manage the inspection policy across each segment of the stack. Click **Edit** to change the segment reference device.
- **Stack Members (N)** — Indicates the number of TippingPoint IPS devices that belong to the stack configuration in the SMS.



Note: For information about the devices that are linked together in the stacking bus, use the **Stack Port A** and **Stack Port B** columns. See [Verify stacking bus state](#) on page 28.

Verify stacking bus state

The **Summary** tab displays stacking bus health by checking the state of the stacking ports and the state of the stack topology on each device. If the status of the stacking bus is not green (normal), identify and resolve any issues.

To verify stacking bus state

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. In the **Summary** tab, verify stacking is enabled on each device and the status of stacking port connectivity:



- **Enabled** — Indicates whether stacking is  enabled or  disabled.



Stacking is automatically enabled when you add a device to the stack. If necessary, remove the device from the stack and then add it to the stack to enable stacking.

- **Stack Port A** and **Stack Port B** — Indicate the stacking port connectivity. See also, [Device shelf-level graphic](#) on page 24.

The following information provides stacking port status information and suggested actions.

Table 3. Stacking port status




Status	Information	Suggested action
 <i>devicename</i>	Indicates the device to which the stacking port is resolved.	No action is required.
 <No Peer>	Indicates a peer device is not connected to the stacking port.	Validate that the stacking port is connected to a stacking port on a peer device. See Install the stacking components on page 4.

Status	Information	Suggested action
	Indicates the peer device that is connected to the stacking port does not have stacking enabled.	Validate that stacking is enabled on the peer device. See View overall health of the stack on page 25.
 <Unknown> (<i>mac-address-hex</i>)	Indicates the peer device that is connected to the stacking port is not managed by the SMS.	Add the peer device to the SMS. See Add the stacking devices to the SMS on page 6.
 No peer information is available	Indicates no stacking information was returned from a peer device.	Verify that the stacking port is connected to the same stacking bus as the segment reference device.

4. Use the **Status** column to verify the *stack topology* state.

The following information provides stack topology status information and suggested actions.

Table 4. Stack topology status

Status	Information	Suggested action
 Segment Reference	Indicates that the device has been designated as the segment reference device and is ready for stacking.	No action is required.
 Normal	Indicates that the device is functioning normally.	No action is required.
 Missing peer	Indicates a peer device is not connected to the stacking port.	Validate that the stacking port is connected to a peer device. See Install the stacking components on page 4.

Status	Information	Suggested action
	Indicates the peer device that is connected to the stacking port does not have stacking enabled.	Validate that stacking is enabled on the peer device.
■ Peer {device-name} is not a stack member	Indicates that a device stacking port references a device that is not actually a part of the stack. This message appears once for each stacking port.	Update the stack configuration to add the device. See Add a device to the stack on page 15.
■ Not in stack	Indicates that the device is not in the stack topology.	Validate that the stacking port is connected to a peer device that is a member of the stack. See Install the stacking components on page 4.
■ No stacking ports	Indicates that the device does not have the required 40 GbE QSFP+ I/O module in slot 4.	Verify that the 40 GbE QSFP+ I/O module is installed in slot 4.
■ Wrong I/O Modules in slot(s) {slot numbers}	Indicates that there is an I/O module on the device that does not match the I/O module in the segment reference device.	Verify that the slot on the device is configured with the same network I/O module or no network I/O module as compared to the segment reference device. See Install the stacking components on page 4.
■ Unknown peer(s) found	The peer device that is connected to the stacking port is not managed by the SMS.	Add the peer device to the SMS. See Add the stacking devices to the SMS on page 6.
	The peer device is not added to the SMS stack configuration.	Add the device to the stack. See Add a device to the stack on page 15.

Verify stack member state






The **Summary** tab displays the state of each stack member as reported by the device. If the status of a stack member is not green (normal), identify and resolve any issues.





To verify stack member state

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. In the **Summary** tab, use the **Stack Member State** column to verify the *stack member* status.

The following information provides stack member status information and suggested actions.

Table 5. Stack member status

Status	Information	Suggested action
 RTI - Normal	Indicates that the stack member is working correctly.	No action is required.
 NRTI - Unknown	Indicates that the stack member is not inspecting traffic for an unknown reason.	This is a transitory state and no action is required.
 NRTI - Rebooting	Indicates that the stack member is not inspecting traffic because it is rebooting.	This is a transitory state and no action is required.
 NRTI - L2FB	Indicates that the stack member is not inspecting traffic because it is stuck in Intrinsic HA L2FB.	At a minimum, reboot the device. If the device returns to this state, a hardware-related issue is likely.
 NRTI - L2FB, Recoverable	Indicates that the stack member is not inspecting traffic because it is waiting for you to disable Intrinsic HA L2FB.	Disable Intrinsic HA L2FB on the stack. See Intrinsic HA on page 44.

Status	Information	Suggested action
 RTI - L2FB	Indicates that the stack member is in Intrinsic HA L2FB but can return to  Ready to Inspect - Normal when the stack master determines that the minimum number of devices are ready to inspect.	Depending on whether you configured the stack for resiliency, all but one of the stack members, or all of the stack members must declare they are  Ready to Inspect - Normal before the stack master returns the stack to  Ready to Inspect - Normal. See Enable or disable stack resiliency on page 12.

Verify device state




The **Summary** tab displays the state of each device. If the status of a device is not green (normal), identify and resolve any issues.




To verify device state

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. In the **Summary** tab, use the **Device State** column to verify the *device* status.

The following information provides device status information and suggested actions.

Table 6. Device status

Status	Information	Suggested action
 Normal	Indicates that the device is working normally.	No action is required.
 Updating	Indicates that the device is updating its status.	This is a transitory state and no action is required.
 Unmanaged	Indicates the device is not managed by the SMS.	In the SMS, manage the device:

Status	Information	Suggested action
		<ol style="list-style-type: none"> a. In SMS tools, click Devices. b. Right-click the unmanaged device and click Edit > Manage Device.
 Not Communicating	Indicates that the device is not communicating across the management network with the SMS.	<p>Verify network connectivity between the SMS and the device. Also, verify the required ports are not blocked.</p> <p>For more information, see the <i>Security Management System User Guide</i>.</p>
 Layer 2 Fallback	Indicates that the device is not inspecting traffic because Intrinsic HA L2FB is enabled.	<p>If you enabled Intrinsic HA L2FB on the device, disable Intrinsic HA L2FB. See Intrinsic HA on page 44.</p> <p>If you cannot disable Intrinsic HA L2FB, determine whether stacking has put the device into Intrinsic HA L2FB. See Verify stack member state on page 31.</p>
 Rebooting	Indicates that the device has started a reboot based on a request from the SMS.	This is a transitory state and no action is required.

Verify stack synchronization

The **Sync Health** tab displays stack synchronization status. For example, synchronization status indicates whether the same TippingPoint Operating System (TOS) version is installed on each device. If the status of the synchronization health is not green (normal), identify and resolve any issues.

There are configuration items that should match across each segment of the stack. For example, virtual segments and segment group membership should be the same. Profiles must be the same on





corresponding segments. If they do not match, the SMS indicates the mismatch and shows the stack health degraded.





To verify stack synchronization









1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.
3. Click the **Sync Health** tab.
4. Use the **Status For** and **Issue** columns to identify synchronization issues.





The following information provides synchronization status information and suggested actions.







Table 7. Stack synchronization status





Stack information	Information	Suggested Action
 TOS	<p>Indicates the TippingPoint Operating System (TOS) version for each of the devices.</p> <p>Critical indicator : Mismatch in versions or distribution.</p> <p>Tip: To filter synchronization information by this type of issue, use the Type column to filter by TOS Versions.</p>	<p>Distribute the TOS version to the stack.</p> <p>Note: For information about where the options are different for managing a stack of devices instead of a single device, see the <i>Security Management System User Guide</i>.</p>
 Digital Vaccine	<p>Indicates the Digital Vaccine (DV) version for each of the devices.</p> <p>Major indicator : Mismatch in versions or distribution.</p> <p>Tip: To filter synchronization information by this type of issue, use the Type column to filter by Digital Vaccines.</p>	<p>Distribute the DV package to the stack.</p> <p>Note: For information about where the options are different for managing a stack of devices instead of a single device, see the <i>Security Management System User Guide</i>.</p>


Stack information	Information	Suggested Action
 {aux-dv-sub type-name} ThreatDV	<p>Indicates the ThreatDV version of a specific ThreatDV subtype for each of the devices. If a ThreatDV subtype has not been distributed to a device, the cell value is <None>.</p> <p>Major indicator : Mismatch in versions or distribution.</p> <p>If a ThreatDV subtype is not distributed to any devices, it is not displayed.</p> <p>Tip: To filter synchronization information by this type of issue, use the Type column to filter by ThreatDV Versions.</p>	<p>Distribute the ThreatDV package to the stack.</p> <p>Note: For information about where the options are different for managing a stack of devices instead of a single device, see the <i>Security Management System User Guide</i>.</p>
 {dvt-name}	<p>Indicates the Digital Vaccine Toolkit (DVT) version of a specific DVT for each of the devices. If a DVT has not been distributed to a device, the cell value is <None>.</p> <p>Major indicator : Mismatch in distributions (not versions).</p> <p>If a DVT is not distributed to any devices, it is not displayed.</p> <p>Tip: To filter synchronization information by this type of issue, use the Type column to filter by DVToolkit Versions.</p>	<p>Distribute the DVToolkit package to the stack.</p> <p>Note: For information about where the options are different for managing a stack of devices instead of a single device, see the <i>Security Management System User Guide</i>.</p>

Stack information	Information	Suggested Action
 { <i>physical-segment-name-and-direction</i> }	<p>Indicates  {<i>profile name</i>} {<i>profile-version</i>} for each of the devices.</p> <p>Major indicator : Mismatch between profile name, profile version, or distribution.</p> <p>Major indicator : <Unknown> A profile has not been distributed to a segment on one of the devices.</p> <p>Tip: To filter synchronization information by this type of issue, use the Type column to filter by Physical Segment's Profiles.</p>	<p>Distribute the profile to the stack.</p> <p>Note: For information about where the options are different for managing a stack of devices instead of a single device, see the <i>Security Management System User Guide</i>.</p>
 { <i>virtual-segment-name</i> }	<p>Indicates the  {<i>profile-name</i>} {<i>profile-version</i>} was distributed to a virtual segment on each of the devices.</p> <p>Major indicator : <Unknown> A profile has not been distributed to a virtual segment on any device, or a profile exists but it was not distributed by the SMS.</p> <p>Major indicator : Mismatch between profile name, profile version, or distribution is displayed. There is one row for each virtual segment.</p>	<p>Distribute the profile to the stack.</p> <p>Note: For information about where the options are different for managing a stack of devices instead of a single device, see the <i>Security Management System User Guide</i>.</p>

Stack information	Information	Suggested Action
	<p>Tip: To filter synchronization information by this type of issue, use the Type column to filter by Virtual Segment's Profiles.</p>	
 {virtual-segment-name}	<p>Indicates a virtual segment exists on the SRD but is missing from all the other stack members.</p> <p>Critical indicator : There is one missing virtual segment row for each virtual segment on the SRD that is not on any of the other member devices.</p> <p>Tip: To filter synchronization information by this type of issue, use the Type column to filter by Missing Virtual Segment.</p>	<p>Edit and save the virtual segment to update the stack.</p> <p>Note: For information about where the options are different for managing a stack of devices instead of a single device, see the <i>Security Management System User Guide</i>.</p>
 {virtual-segment-name}	<p>Indicates an extra virtual segment exists on one of the stack members but is missing from the SRD.</p> <p>Critical indicator : There is one extra virtual segment row for each virtual segment that is not in the segment reference device but is in one of the other devices in the stack.</p> <p>Tip: To filter synchronization information by this type of issue, use</p>	<p>Delete the extra virtual segment if it is not applicable. Or, edit and save the virtual segment to update the stack.</p> <p>Note: For information about where the options are different for managing a stack of devices instead of a single device, see the <i>Security Management System User Guide</i>.</p>

Stack information	Information	Suggested Action
	<p>the Type column to filter by Extra Virtual Segment.</p>	
<p> {virtual-segment-name}</p>	<p>Indicates the  {segment-group-name} to which a virtual segment belongs for each of the devices.</p> <p>Critical indicator : Mismatch displayed.</p> <p>There is one row for each virtual segment that has a mismatch in segment groups.</p> <p>Tip: To filter synchronization information by this type of issue, use the Type column to filter by Virtual Segment's Group.</p>	<p>Edit and save the segment group (without making any changes) to update the segment group with all of its segments.</p> <p>Note: For information about where the options are different for managing a stack of devices instead of a single device, see the <i>Security Management System User Guide</i>.</p>
<p> {physical-segment-name}</p>	<p>Indicates the  {segment-group-name} to which a physical segment belongs for each of the devices.</p> <p>Critical indicator : Mismatch displayed.</p> <p>There is one row for each physical segment that has a mismatch in segment groups.</p> <p>Tip: To filter synchronization information by this type of issue, use the Type column to filter by Physical Segment's Group.</p>	<p>Edit and save the segment group (without making any changes) to update the segment group with all of its segments.</p> <p>Note: For information about where the options are different for managing a stack of devices instead of a single device, see the <i>Security Management System User Guide</i>.</p>

Stack information	Information	Suggested Action
 {inspection-bypass-rule-name}	<p>Indicates an inspection bypass rule is missing from the SRD but exists on a device in the stack.</p> <p>Critical indicator : Mismatch displayed.</p> <p>There is one row for each inspection bypass rule that does not exist on the segment reference device but exists on a device in the stack.</p> <p>Tip: To filter synchronization information by this type of issue, use the Type column to filter by Missing Inspection Bypass Rule.</p>	<p>Edit and save the inspection bypass rule (without making any changes) to update the stack.</p> <p>Note: For information about where the options are different for managing a stack of devices instead of a single device, see the <i>Security Management System User Guide</i>.</p>
 {inspection-bypass-rule-name}	<p>Indicates an extra inspection bypass rule exists on the SRD but is missing from a device in the stack.</p> <p>Critical indicator : Mismatch displayed.</p> <p>There is one row for each inspection bypass rule that is missing from a device in the stack but exists on the SRD.</p> <p>Tip: To filter synchronization information by this type of issue, use the Type column to filter by Extra Inspection Bypass Rule.</p>	<p>Edit and save the inspection bypass rule (without making any changes) to update the stack.</p> <p>Note: For information about where the options are different for managing a stack of devices instead of a single device, see the <i>Security Management System User Guide</i>.</p>



Stack information	Information	Suggested Action
Stack Resilience { <i>stack-resilience-value</i> }	<p>Indicates that there is at least one device that has a different Stack Resilience option than what is configured for the stack in the SMS.</p> <p>Critical indicator : Mismatch displayed.</p> <p>Tip: To filter synchronization information by this type of issue, use the Type column to filter by Device Resilience Mismatch.</p>	Edit and save the stack configuration (without making any changes) to update all of the stacking devices.

Resolve issues adding a device to the stack

The following information describes how to identify and resolve issues with adding a device to the stack configuration in the SMS.

The following information provides device status and suggested actions for adding a device to the stack.

Table 8. Device status – adding a device to the stack

Status	Information	Suggested action
 Ready for stacking	Indicates that there is no issue with adding the device to the stack.	No action is required.
 No QSFP+ module in slot 4	Indicates that the device does not have the required I/O module in slot 4.	Verify the 40 GbE QSFP+ I/O module is properly installed in slot 4. If necessary, reboot the device.

Status	Information	Suggested action
<p>■ This device's model doesn't match the model for the selected devices.</p>	<p>Indicates that there is a device model mismatch.</p>	<p>Select devices that are either all 7500NX or all 7100NX.</p>
<p>■ This device's TOS version doesn't match the TOS version for the selected devices.</p>	<p>Indicates that there is a TOS version mismatch.</p>	<p>The TippingPoint Operating System (TOS) version must be the same on each device in the stack. If necessary, install a matching TOS version on the device and then add it to the stack.</p>
<p>■ This device does not support stack sizes of more than ## devices.</p>	<p>Indicates a device is valid for stacking, but that the maximum number of devices in the stack has been reached.</p>	<p>Remove a device from the stack so that you can add the device.</p> <p>See Remove a device from the stack on page 14.</p>
<p>■ Device is not communicating</p>	<p>Indicates that the device is not communicating with the SMS.</p>	<p>Verify network connectivity between the SMS and the device. Also, verify the required ports are not being blocked.</p> <p>For more information, see the <i>Security Management System User Guide</i>.</p>
<p>■ Device is unmanaged</p>	<p>Indicates that the device is no longer managed by the SMS.</p>	<p>In the SMS, manage the device:</p> <ol style="list-style-type: none"> 1. In SMS tools, click Devices. 2. Right-click the unmanaged device and click Edit > Manage Device.

View stacking tier statistics

In the SMS, use the stacking tier statistics to view stacking (Tier S) data for a stacking device in addition to device tiers 1–4. Tier S data includes stacking data from the stacking ports and the 40 GbE QSFP+ I/O module.

The tier statistics area provides information on packets and speed as measured in Mbps by tier.

Inspection Tier	Information
Stack : Segment Ports	<p>This inspection tier presents the total I/O module throughput for the network segment device as well as the receive rates from the I/O module to each stack member.</p> <p>When stacking is enabled, the following information is displayed:</p> <ul style="list-style-type: none"> • Segment Rx Mbps displays the aggregate received traffic from all network segments on this device. • Segment Tx Mbps displays the aggregate traffic transmitted from all network segments on this device. • Stack Balance (A/B/C) displays the load balance percentage, in which 100% equates to perfect balance across the number of devices in the stack. For devices that are in Intrinsic HA L2FB, the Rx rate is zero, and this zero value is included in the load balance calculation. This statistic is similar to the A/B/C Balance percentage in Tier 1. <ul style="list-style-type: none"> ◦ <host n> Rx Mbps displays the traffic balanced from this device's network segments to the other devices in the stack. <p>Note that the number of packets going through each host is flow-based, so it is not uncommon to see a slight difference between them.</p> • Segment ratio to tier 1 displays the percentage of traffic being inspected by this device as a ratio of the segment Rx traffic.
Stack : Stack Ports	<p>This inspection tier presents stacking port throughput, including through traffic and return traffic rates.</p> <p>When stacking is enabled, the following information is displayed:</p> <ul style="list-style-type: none"> • Stack Rx Mbps displays the aggregate received traffic from both stacking ports.

Inspection Tier	Information
	<ul style="list-style-type: none"> Stack Tx Mbps displays the aggregate traffic that is transmitted from both stacking ports. Stack Rx > Stack Tx displays the total amount of transit or through traffic on the stacking ports; for example, traffic received on Stack port 1, which is forwarded by the switch to stack port 2. Stack Rx > Seg Tx displays the amount of return traffic coming in on a stacking port that is returning to the outbound network segment. Stack ratio to tier 1 displays the percentage of traffic being inspected by this device as a ratio of the stack Rx traffic.

For more information, see the *Security Management System User Guide*.

Enable or disable Intrinsic High Availability Layer-2 Fallback

Intrinsic High Availability (Intrinsic HA) determines how the device manages traffic on each segment in the event of a system failure. Layer-2 Fallback (L2FB) mode either permits or blocks all traffic on each segment, depending on the Intrinsic HA L2FB action setting for the segment. Any permitted traffic is not inspected.

In the SMS, you can enable Intrinsic HA L2FB on a stack member or the entire stack, for example, to perform scheduled maintenance. When you finish, disable Intrinsic HA L2FB to resume normal operation.

Stacking automatically enables and disables Intrinsic HA L2FB on a stack member or the stack as needed, depending on the inspection state of the stack or the devices.

- *Ready to Inspect (RTI)* indicates that a device or the stack is ready to inspect traffic. If enough devices are RTI, the stack master takes the stack out of Intrinsic HA L2FB. See [Enable or disable stack resiliency](#) on page 12.
- *Not Ready to Inspect (NRTI)* indicates that a device or the stack is not ready to inspect traffic.

When a device or stack is NRTI, Intrinsic HA L2FB remains enabled until the NRTI cause is resolved. In some cases, NRTI is a temporary recoverable condition and in other cases, NRTI recovery requires manual intervention. See [Verify stack member state](#) on page 31.

Tip: If a device or the stack is in Intrinsic HA L2FB, disable Intrinsic HA L2FB on the stack to restore the stack to Normal mode. If the stack does not return to Normal mode, verify the

stack health to determine why the stack is in Intrinsic HA L2FB and resolve any issues. See [Verify stack health and synchronization](#) on page 25.

Enable or disable Intrinsic HA L2FB on the stack

In the SMS, enable Intrinsic HA L2FB mode on the stack to either permit or block all traffic on each segment of the devices in the stack, depending on the Intrinsic HA L2FB action setting for the segment. When you disable Intrinsic HA L2FB on the stack, any devices in Intrinsic HA L2FB are restored to Normal mode.

To resume normal operation, the stack must validate:

- The minimum number of devices are RTI - Normal. See [Verify stack health and synchronization](#) on page 25.
- The stack members communicate regularly with the stack master.

If the number of missed heartbeats exceeds a threshold value, or if the device does not send a heartbeat message within 15 minutes of rebooting, the device is NRTI.

- The same TippingPoint Operating System (TOS) version is installed on each device. See [Verify stack synchronization](#) on page 33.

If you manually enable Intrinsic HA L2FB on the stack, you must also disable it to resume inspection. If necessary, resolve Intrinsic HA L2FB issues on a device to bring the stack out of Intrinsic HA L2FB.

To enable or disable Intrinsic HA L2FB on the stack

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, right-click the stack and click **Edit > Intrinsic HA**, then choose an option:
 - **Fallback** puts the stack in Intrinsic HA L2FB.
 - **Normal** takes the stack out of Intrinsic HA L2FB.

Enable or disable Intrinsic HA L2FB on a stacking device

In the SMS, enable Intrinsic HA L2FB mode on a stacking device to either permit or block all traffic on each segment, depending on the Intrinsic HA L2FB action setting for the segment. When you disable Intrinsic HA L2FB on the device, Intrinsic HA L2FB is restored to Normal mode.

Before you enable Intrinsic HA L2FB on a stacking device, verify whether the loss of the device would place the entire stack into Intrinsic HA L2FB. See [Enable or disable stack resiliency](#) on page 12.

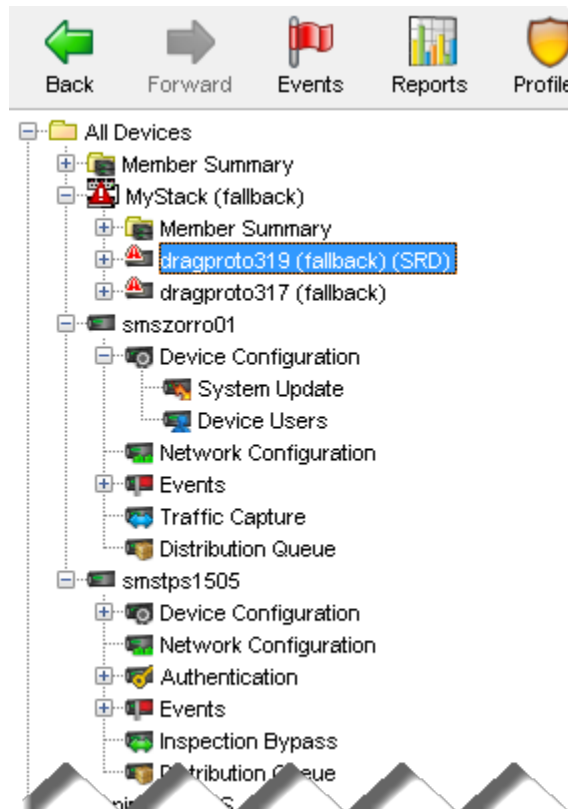
To enable or disable Intrinsic HA L2FB on the stacking device

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, double-click the stack.

3. In the left navigation pane, expand the stack.

If a stacking device is in Intrinsic HA L2FB, the name of the device is appended by **(fallback)**. In the following example, **MyStack** and its stack members are in Intrinsic HA L2FB.

Figure 11. Stack in Intrinsic HA L2FB



4. Click the device that is in Intrinsic HA L2FB.
The stacking device shelf-level graphic is displayed.
5. In the **Device** workspace, right-click the shelf-level graphic and click **Edit > Intrinsic HA**, then choose an option:
 - **Fallback** puts the device in Intrinsic HA L2FB.
 - **Normal** takes the device out of Intrinsic HA L2FB.

Export a Tech Support Report from an IPS device

In the SMS, you can collect diagnostic information from an IPS device by exporting a Tech Support Report (TSR). The TSR collects information from diagnostic commands and log files into a report that TippingPoint Technical Support can use to debug and troubleshoot the device.

Unlike a TSR created on the device by using the IPS Local Security Manager, the TSR exported by the SMS does not include snapshot information. However, you can create a snapshot from the SMS.

For more information about creating a TSR from the IPS Local Security Manager, see the *Local Security Manager User Guide*.

Important: The SMS exports a TSR from TippingPoint IPS devices only. To create a TSR for another type of TippingPoint security device, use the Local Security Manager.

To collect diagnostic information for the stack

1. Use the SMS to export a TSR from each TippingPoint IPS in the stack.
2. After the report is created, you can save it to your local system.
3. You can then email the file to TippingPoint Technical Support for assistance. For contact information, go to <https://tmc.tippingpoint.com>.

To create a Tech Support Report

1. In the SMS tools, click **Devices**.
 - If the device is not a member of a stack:
 - a. In the **All Devices** workspace, right-click the shelf-level graphic for the standalone IPS and select **Export TSR**.

Note that TSR export is only available for IPS devices, not TPS devices.
 - b. Click **Export** to download a `tar.zip` file of the report to your local Downloads directory.
 - If the device is a member of a stack:
 - a. In the **All Devices** workspace, double-click the stack.
 - b. In the left navigation pane, expand the stack to select the stacking device.
 - c. Right-click the shelf-level graphic for the stacking device and select **Export TSR**.
 - d. Click **Export** to download a `tar.zip` file of the report to your local Downloads directory.

CLI commands for stacking

On the IPS, use the Command Line Interface (CLI) to display stacking status information from the device. For more information about stacking-related commands, see the *IPS Command Line Interface Reference*.

show stacking

Enter this command to show stacking status information.

Required privilege

Admin, Operator, Super-User

Use

The following example shows the default output for a device that does not support stacking. To support stacking, the device must be a supported model running TippingPoint Operating System (TOS) v3.9.0 (or later).

```
ips# show stacking
This device does not support stacking.
```

The following example shows the default output for a supported device that is not a member of the stack. Unlike the SMS, the device does not validate the presence of the 40 GbE QSFP+ NX module in slot 4.

```
ips# show stacking
Stack member summary
-----
Stacking enabled           : No
Stacking active           : No
Stack member state        : Device Ready to Inspect - Normal
Stack master              : No
```

The following example shows the output for the same device after adding it to a stack of three devices.

```
ips# show stacking
Stack member summary
-----
Stacking enabled           : Yes
Stacking active           : Yes
Stack member state        : Device Ready to Inspect - Normal
Stack master              : No
Stack summary
-----
Number of devices configured in stack : 3
Number of devices required in stack   : 2
Stack state                   : Stack Ready to Inspect - Normal
Device Hostname               Advertised State
-----
device01 (local host)         Device Ready to Inspect - Normal
device02 (master)             Device Ready to Inspect - Normal
device03                       Device Ready to Inspect - Normal
```

Reference

Parameter	Information
Stacking enabled	Indicates whether stacking is enabled on the device.

Parameter	Information
Stacking active	Indicates whether stacking is currently functioning.
Stack member state	Indicates the current working state of this device on the stack.
Stack master	Indicates whether this device manages the state of the stack.
Number of devices configured in stack	Indicates the number of TippingPoint IPS devices that are connected together through the stacking bus.
Number of devices required in stack	Indicates the minimum number of devices that must be available to the stack for normal operation. If the number of normal devices falls below this threshold, the stack goes into Intrinsic HA L2FB.
Advertised state	Indicates the state that the device advertises to the stack master.

Limitations

When you consider stacking, keep these points in mind:

- The following options, which require state information to be shared across multiple devices, are not supported in a stacking configuration:
 - Transparent HA
 - IPS Quarantine. As a workaround, use SMS Responder to propagate IPS Quarantine to stack members.

Note: For information about the differences between configuring a stack of devices compared with configuring a standalone device, see the *Security Management System User Guide*.

- Scan/sweep filters
- Policy-based rate limits
- The SMS is required to manage the stack and any stack members. You cannot manage the stack from the Local Security Manager (LSM) or CLI on the device.
- When stacking is enabled, do not make the following configuration changes to the slot 4 I/O module segments:
 - Enable link-down synchronization
 - Configure VLAN translation rules
 - Configure inspection bypass rules
 - Enable and disable ports
- All stack members must use consistent sets of inspection profiles to ensure inspection policies are applied consistently, regardless of which device inspects the traffic.

Repurpose a device

If you have existing TippingPoint 7100NX or 7500NX devices that are not currently deployed in your network, you can repurpose the devices for use in a stack. Also, if you remove a device from a stack, you can repurpose it for use in another stack or as a standalone device.

For information about adding a device to the stack, see [Add a device to the stack](#) on page 15.

To repurpose a device

- Use the `debug factory-reset` command to restore the device to its original settings.

Keep the following items in mind when you repurpose a device for use in a stack:

- The same TippingPoint Operating System (TOS) version, v3.9.0 or later, must be installed on each NX Series device in the stack.
- A 40 GbE QSFP+ I/O module must be installed in slot 4. If another type of I/O module is installed in slot 4, replace the module. The process is:
 - a. Replace the existing I/O module with the 40 GbE QSFP+ I/O module.
 - b. Use the `reboot -full` command to reboot the device. See the *IPS Command Line Interface Reference* for more information.

Stacking terminology

AOC cable

The *AOC cable* is the TippingPoint 40G QSFP+ Active Optical Cable (AOC) that directly connects a stacking port on a stack member to a stacking port on another stack member.

Intrinsic HA

Intrinsic High Availability (Intrinsic HA) determines how the device manages traffic on each segment in the event of a system failure. If the device fails, the device goes into Layer-2 Fallback (L2FB) mode and either permits or blocks all traffic on each segment, depending on the Intrinsic HA L2FB action setting for the segment. If the Intrinsic HA L2FB action on a segment permits traffic, the traffic is not inspected but is allowed to pass through the segment.

In a stack configuration, the stack determines how to manage Intrinsic HA L2FB in the event of a system failure. If a stack member fails, that device goes into Intrinsic HA L2FB and either permits or blocks all traffic on each segment, depending on how you configured the Intrinsic HA L2FB action setting for that segment. Depending on the stack configuration, the stack can continue to operate normally in the event that one of its members go into Intrinsic HA L2FB, or the stack can be configured to go into Intrinsic HA L2FB.

A TippingPoint administrator can also manually place the stack or a particular stack member into Intrinsic HA L2FB.

See [segment reference device](#) on page 52.

network segment

A *network segment* is created by joining an Ethernet pair of interfaces on the appliance to allow traffic flow and inspection. Segments have an A and B port.

network segment device

A *network segment device* operates in-line in the network and distributes network traffic to each stack member for inspection.

Not Ready to Inspect (NRTI)

Not Ready to Inspect (NRTI) indicates that a device or the stack is not ready to inspect traffic. Note that stacking places a device or stack that is NRTI into Intrinsic HA L2FB until the NRTI cause is resolved. In some cases, NRTI is a temporary recoverable condition and in other cases, NRTI recovery requires manual intervention.

See also [Intrinsic HA](#) on page 51 and [stack resiliency](#) on page 52.

Ready to Inspect (RTI)

Ready to Inspect (RTI) indicates that a device or the stack is ready to inspect traffic. Note that stacking takes a device out of Intrinsic HA L2FB when the NRTI cause is resolved. If enough devices are RTI, the stack master takes the stack out of Intrinsic HA L2FB.

See also [Intrinsic HA](#) on page 51 and [stack resiliency](#) on page 52.

segment reference device

The *segment reference device* (SRD) is the network segment device that the SMS uses as a template to create the corresponding segments on each stack member. *See also* [network segment device](#) on page 51.

stack master

The *stack master* is a device role that is responsible for managing stack configuration and states. The stack master is automatically elected by the devices in the stack. All stack members are eligible for election to stack master.

stack resiliency

A *resilient stack* configuration enables the stack to continue to inspect network traffic if a single stack member is NRTI. If a single stack member is NRTI, the stack rebalances network traffic between the remaining RTI devices, reducing inspection capacity.

stacking

Stacking enables you to group multiple security devices and pool their resources to increase overall inspection capacity. With TippingPoint IPS Stacking, you can configure up to five NX Series security devices in a stack. In-line inspection capacity increases with each device that you add to the stack.

stacking bus

The *stacking bus* consists of a 40 GbE QSFP+ I/O module on each stacking device that connects the stack in a ring topology. Stacking requires the 40 GbE QSFP+ I/O module to be installed in slot 4.

stacking port

A *stacking port* connects each stack member to its peer in a stacking bus. The 40 GbE QSFP+ I/O module, when installed in slot 4, provides two stacking ports. Use an Active Optical Cable (AOC) to directly connect the stacking port on the device to another device. Do not connect the stacking ports through a switch.



TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM37549/160824