



Trend Micro™ TippingPoint™

Threat Protection System (TPS)

Stacking User Guide

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

<https://docs.trendmicro.com/en-us/tippingpoint/threat-protection-system.aspx>

Trend Micro, the Trend Micro t-ball logo, TippingPoint, and Digital Vaccine are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2024. Trend Micro Incorporated. All rights reserved.

Document Part No.: TPEN09848/230927

Release Date: April 2024

Protected by U.S. Patent No.: Pending

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

<https://www.trendmicro.com/download/documentation/rating.asp>

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that TippingPoint Threat Protection System collects and provides detailed instructions on how to disable the specific features that feedback the information.

<https://success.trendmicro.com/data-collection-disclosure>

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

<https://www.trendmicro.com/privacy>

Table of Contents

Chapter 1: TPS Stacking User Guide

Chapter 2: Setting up the stack

Stacking components	2-2
Basic stack configuration	2-2
Install the stacking components	2-3
Create the stack	2-5
Manage the devices	2-5
Create the stack configuration	2-5
Distribute the inspection profile	2-7
Resilient stack configuration	2-8
Multiple network segment devices	2-10

Chapter 3: Updating the stack configuration

Enable stack resiliency	3-3
Change the segment reference device	3-3
Replace a device in the stack	3-4
Remove a device from the stack	3-5
Add a device to the stack	3-6
Delete the stack	3-7
Granting permissions to the stack	3-8
Add stack management to the user role	3-8
Grant the user group access to the stack	3-9
Distribute a TOS update	3-9
Differences between configuring a stack and a standalone device	3-10
Security policy configuration	3-10

Events and reports	3-14
System updates and snapshots	3-15
SMS database restore to a different SMS	3-16

Chapter 4: Troubleshooting

Verify AOC cable installation	4-2
View stacking status	4-3
Device details	4-3
Front panel stacking LEDs	4-6
Device shelf-level graphic	4-7
Verify stack health and synchronization	4-7
View overall health of the stack	4-8
Verify stacking bus state	4-11
Verify stack member state	4-14
Verify device state	4-15
Verify stack synchronization	4-17
Resolve issues adding a device to the stack configuration	4-28
View stacking tier statistics	4-28
Intrinsic HA Layer-2 Fallback	4-30
Enable Layer-2 Fallback on the stack	4-31
Enable Layer-2 Fallback on a stacking device	4-32
Export a Tech Support Report	4-33
CLI commands for stacking	4-34

Chapter 5: Considerations

Chapter 6: Repurposing a device

Chapter 1

Overview

Stacking enables you to increase the overall inspection capacity of your Trend Micro™ TippingPoint™ Threat Protection System (TPS) security device by grouping multiple TX Series or TXE Series devices and pooling their resources.



Note

For expediency, the device graphics in this guide illustrate stacking TX devices. Stack configurations for 9200TXE devices and for 8600TXE devices follow the same guidelines you would use for stacking the 8200TX device; the I/O slot numbers for both of these 1U models correspond.

You can configure up to five devices in a stack. The stack operates as a single device that you manage on the TippingPoint Security Management System (SMS). For a stack of TX Series devices, the devices can be the same or a mixture of both 8200TX and 8400TX TPS models. For a stack of TXE Series devices, the devices must be either 8600TXE devices or 9200TXE devices, but not a mixture of both. All devices in a stack should be licensed for the same inspection throughput.

In-line inspection capacity increases with each device that you add to the stack. For example, for each 8200TX or 8400TX added to a stack of devices, the inspection capacity increases according to the licensed inspection capacity of each device, up to a stacking maximum of 120 Gbps.



Important

Before you attempt to configure a stack, make sure you install the following TippingPoint software:

- For TX Series stacks, TippingPoint Operating System (TOS) v5.0.0 or later for the SMS to centrally manage each stack of devices, and TOS v5.0.3 or later for each security device in the stack.
- For 9200TXE Series stacks, TOS v6.0 or later for both the SMS and TPS devices.
- For 8600TXE Series stacks, TOS v6.3 or later for both the SMS and TPS devices.
- All devices in a stack must be running the same TOS version.



Note

No additional licensing is required to implement stacking.

Not all TPS features are supported in a stack configuration. [Learn more on page 5-1.](#)

Chapter 2

Setting up the stack

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. [Learn more on page 2-8.](#)

For information about how to install your security device, consult the *Read Me First* and *Threat Protection System (TPS) Hardware Specification and Installation Guide*.

Stacking components

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

- For TX Series stacks:
 - TippingPoint 8200TX or 8400TX device
 - TippingPoint 40G QSFP+ Active Optical Cable (AOC) or discrete QSFP+ Transceivers and Cables
- For TXE Series stacks:
 - TippingPoint 9200TXE device or 8600TXE
 - TippingPoint 100G QSFP28-DD Active Optical Cable (AOC) or discrete 100G QSFP28-DD Transceivers and Cables

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.



Important

Before you attempt to configure a stack, make sure you install the following TippingPoint software:

- For TX Series stacks, TippingPoint Operating System (TOS) v5.0.0 or later for the SMS to centrally manage each stack of devices, and TOS v5.0.3 or later for each security device in the stack.
 - For 9200TXE Series stacks, TOS v6.0 or later for both the SMS and TPS devices.
 - For 8600TXE Series stacks, TOS v6.3 or later for both the SMS and TPS devices.
-

Install the stacking components

A TPS device stack consists of two or more devices that connect through a stacking bus.

The **stacking bus** consists of a pair of dedicated 40 GbE QSFP+ (TX Series) or 100G QSFP28-DD ports (TXE Series) on each stacking device. These special purpose (SP) ports directly connect each stack member to its peer by using AOC or QSFP+ cables. Do not connect the SP ports through a switch.



Note

For expediency, the device graphics in this guide illustrate stacking TX devices. Configurations for stacking the 9200TXE or 8600TXE devices follow the same guidelines you would use for stacking the 8200TX device; the I/O slot numbers for both of these 1U models correspond.

To install the stacking components

Procedure

1. Install the I/O modules 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.



Note

If you have a mixed stack configuration with 8400TX and 8200TX devices, maximize the physical network I/O slots that are available to the stack by installing network I/O modules in any of the network I/O slots on the 8400TX security device.

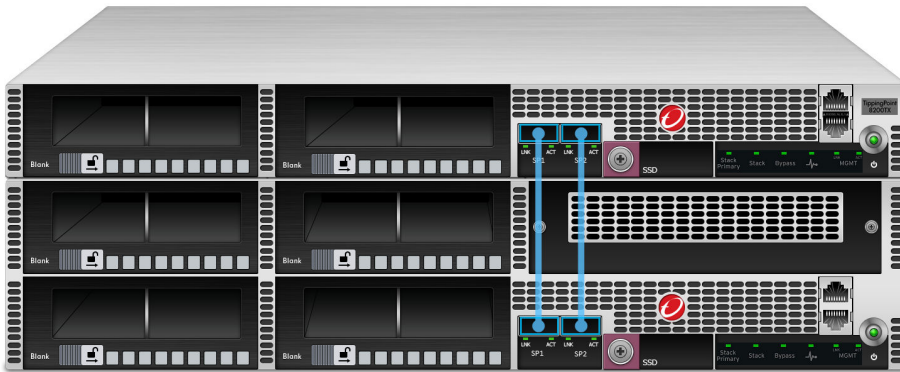
For information about how to install I/O modules, see the *Threat Protection System (TPS) Hardware Specification and Installation Guide*.

2. Install the AOC or QSFP+ (for TXSeries)/QSFP28-DD (for TXE Series) cables in the SP ports 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 transceiver with the tab **on top**. There is only one way to correctly insert the AOC cable. If the cable does not slide in easily and click to latch, it may be upside down. [Learn more on page 4-2](#).

The following example shows a mixed stack configuration with an 8400TX (bottom) and an 8200TX (top) security device. The AOC cables are properly installed in the SP ports.



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



Create the stack

Create the stack configuration in the SMS to centrally manage your installed stacking devices.

Complete these tasks to create the stack:

- [Manage the devices on page 2-5](#)
- [Create the stack configuration on page 2-5](#)
- [Distribute the inspection profile on page 2-7](#)

Manage the devices

Manage the devices that you want to stack with the SMS so that you can create and manage the stack.

For each device, install the required TOS version. The TOS version must be the same on each TPS device.

If you are repurposing an existing device for use in the stack, verify the device configuration. [Learn more on page 6-1.](#)

Create the stack configuration

Create the stack configuration to specify the devices that are connected to the stacking bus and the Devices options.



Note

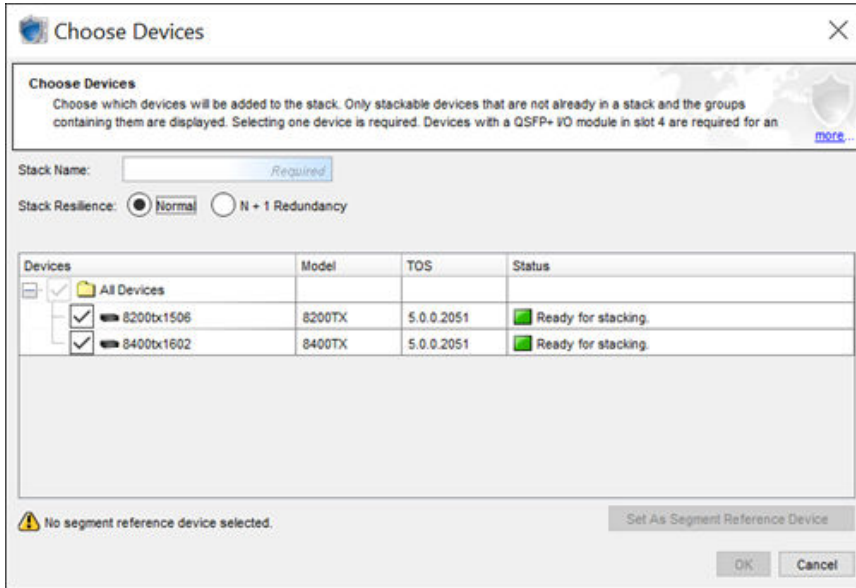
You must have a SuperUser role for SMS administration to create a stack.

To create a basic stack with two devices


Procedure

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** dialog, specify the stack name.



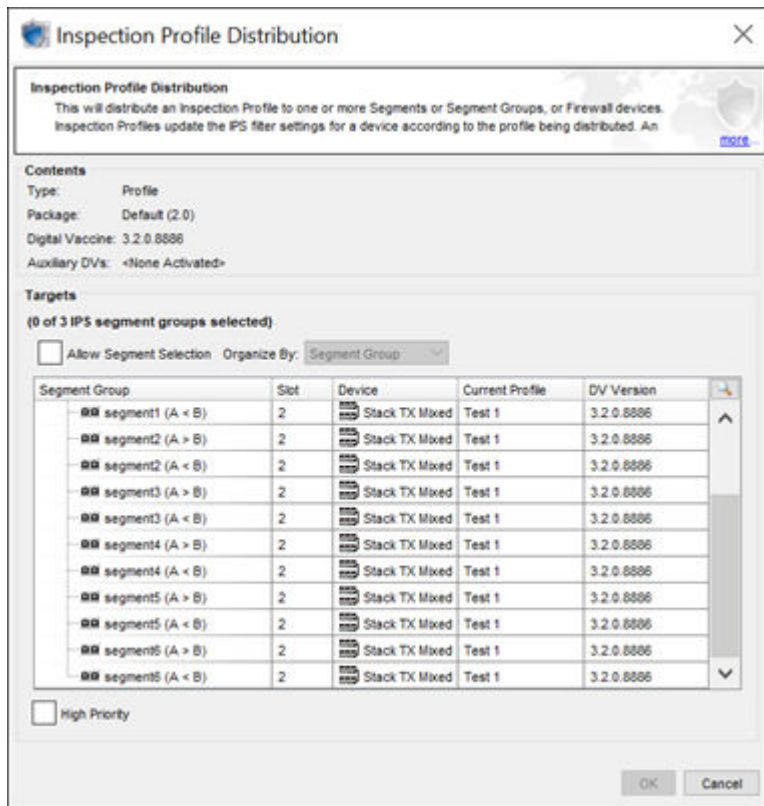
4. Choose **Normal** for the Stack Resilience option.
5. Select both devices.
 - If a device is not displayed, validate the following items:
 - The device is not already a member of another stack.
 - The device is either a TX Series (8200TX or 8400TX) or TXE Series TPS.
 - If either device does not have a **Ready for stacking** status, troubleshoot the issue.
6. Select the device with network I/O modules and click **Set as Segment Reference Device**. Stacking replicates the I/O module configuration of the segment reference device to the other stack members.
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.
-

Distribute the inspection profile

Distribute the inspection profile to the stack by choosing from the network segments on the segment reference device. The SMS distributes the inspection profile to the corresponding segments on each member of the stack.

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



After you distribute the inspection profile, use the **Sync Health** tab to identify and resolve any synchronization issues with the stack. [Learn more on page 4-17.](#)

Resilient stack configuration

You can change the configuration of a basic stack to a resilient stack. In a *resilient stack*, the network traffic continues to be inspected when a single

stack member is not ready to inspect by rebalancing network traffic between the remaining devices that are ready to inspect.

To enable a resilient stack configuration, follow the same process that is described in [Create the stack configuration on page 2-5](#), but select the **N+1 Redundancy** Stack Resiliency option.

When all the devices in the stack are ready to inspect, the stack balances network traffic across all the devices. If a single stack member is not ready to inspect, the stack balances network traffic between the remaining devices, reducing inspection capacity.



Important

When the stack is configured with a single network segment device, if the network segment device is not ready to inspect, the entire stack is not ready to inspect. To enable the stack to continue to inspect traffic when the network segment device is not ready to inspect, configure multiple network segment devices.

The following example shows a resilient stack:

- The network segment device (1) is at the bottom of the stack.
- The network segment device 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.



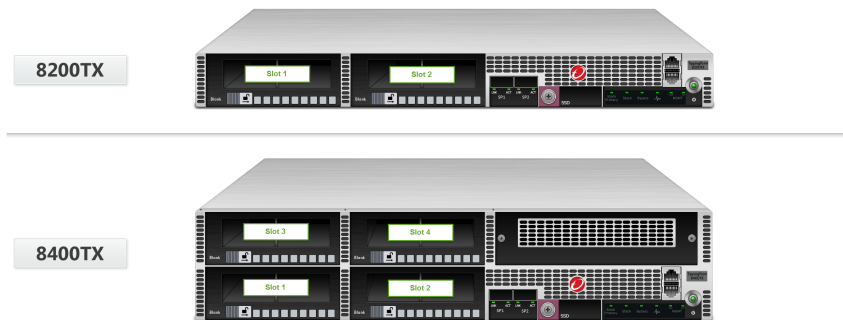
Multiple network segment devices

You can change the device configuration of an **N+1 Redundancy** resilient stack to include multiple network segment devices (NSDs). With more than one NSD, 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.

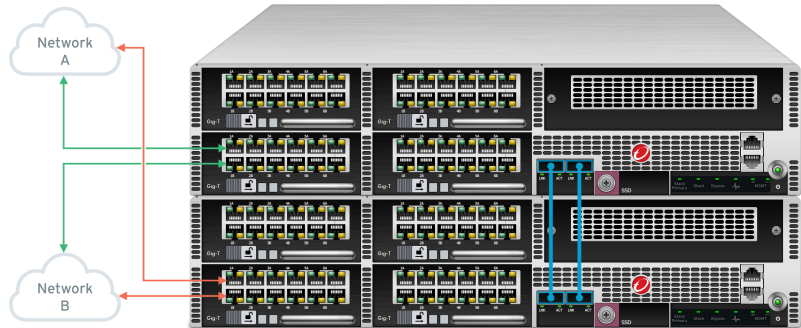
Consider these points when you configure multiple NSDs:

- If you configure multiple NSDs, ensure each network segment device is the same TPS model (for example, either 8200TX or 8400TX, but not both) to prevent configuration issues.
- Configure the **same** slot on each device with either the **same** network I/O module or **no** network I/O module.

The following example shows the slot numbers for 8200TX and 8400TX devices.

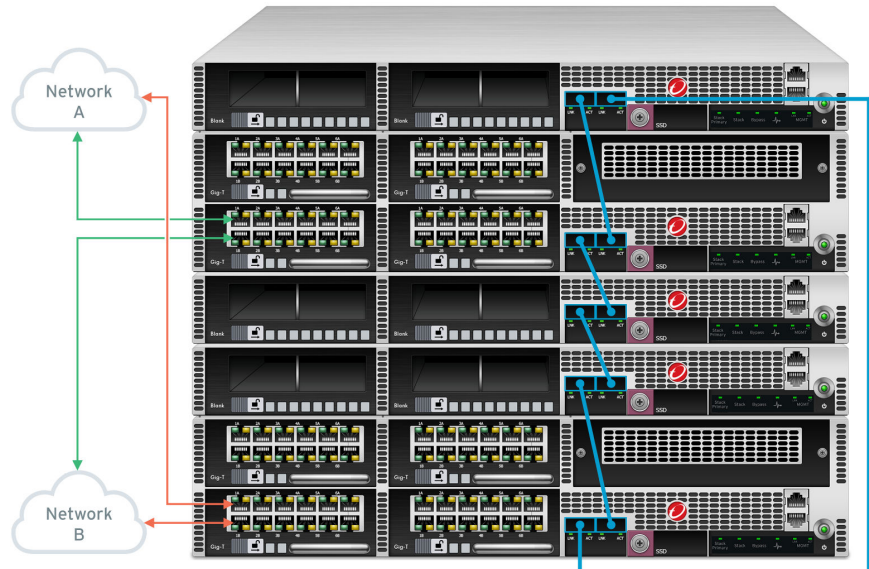


- Traffic can come in both NSDs as long as the corresponding segment ports of each device are connected to the same networks. The next example shows a valid two-device stack where port 1-1A on IPS-A and IPS-B are connected to Network A and port 1-1B on IPS-A and IPS-B are connected to Network B. You can designate either NSD as the segment reference device. Each NSD balances traffic from each utilized segment to the other member of the stack on a per flow basis.



- For stacks of four or five devices, the NSD devices cannot be adjacent to each other.

The next example shows a valid five-device stack where the bottom device and the second device from the top have been designated as the NSDs. Both NSDs must be the same model, and in this example they are 8400TX devices.



- The maximum number of active NSD devices in any stack is two.

Chapter 3

Updating the stack configuration

Update the stack configuration, for example, when you need to add another device to the stack.



Important

Do not reboot all devices in a stack at the same time. When you have to reboot devices in a stack configuration, reboot each device that you updated sequentially. Allow each device to finish the boot sequence completely—ensuring that the SMS has successfully managed the device—before rebooting the next device.

All devices in the stack must be managed and communicating with the SMS when you change any configuration. Otherwise, the stack configuration will get out of sync.

Learn more on page 3-10 about how configuring a stack of devices differs from configuring a standalone device.

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

- *Enable stack resiliency on page 3-3*
- *Change the segment reference device on page 3-3*

- *Replace a device in the stack on page 3-4*
- *Remove a device from the stack on page 3-5*
- *Add a device to the stack on page 3-6*
- *Delete the stack on page 3-7*
- *Granting permissions to the stack on page 3-8*
- *Distribute a TOS update on page 3-9*

Enable stack resiliency

When you enable stack resiliency, make sure the stack is configured with enough devices to provide the required inspection capacity if a single stack member is not ready to inspect. Disable stack resiliency to maximize inspection throughput.

To enable or disable stack resiliency

Procedure

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 not ready to inspect. If more than one device is not ready to inspect, the stack automatically goes into Intrinsic HA Layer-2 Fallback.
 - **Normal** – This option automatically places the stack and all of its devices into Intrinsic HA Layer-2 Fallback if a single stack member is not ready to inspect.
-

Change the segment reference device

Update the stacking configuration to designate a network segment device as the segment reference device.

Stacking replicates the network I/O module configuration of the segment reference device to the other stack members. [Learn more on page 3-3](#).

To change the segment reference device

Procedure

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.
-

What to do next

After you change the segment reference device, distribute the inspection profile to update the stack. [Learn more on page 2-7](#).

Replace a device in the stack

The following information describes how to replace a stacking device.

To replace a device in the stack

Procedure

1. Enable Intrinsic HA Layer-2 Fallback on the stack.
2. Remove the device from the stack configuration. If the device you want to replace is the segment reference device, temporarily designate another device as the segment reference device. You cannot remove a device from the stack configuration while it is the segment reference device.
 - a. In the SMS tools, click **Devices**.
 - b. In the **All Devices** workspace, double-click the stack.
 - c. In the **Summary** tab, select a device from the Stack Member list.
 - d. Click **Remove**.
3. Install the replacement device in your rack and install the AOC or QSFP+ cables to connect the replacement device to the stacking bus.

4. If you need to replace any network I/O modules, install the same I/O modules in the same slots of the replacement device.
5. Manage the new device with the SMS and then add the stacking device to the stack configuration.

If necessary, update the stack configuration to designate the replacement device as the segment reference device.

6. Distribute the inspection profile to the stack.
 7. Disable Intrinsic HA Layer-2 Fallback on the stack.
-

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.



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 has a degraded health status.

To remove a device from the stack

1. Enable Intrinsic HA Layer-2 Fallback on the stack.
2. Remove the stack member from the stack configuration.
 - a. In the SMS tools, click **Devices**.
 - b. In the **All Devices** workspace, double-click the stack.
 - c. In the **Summary** tab, select a device from the Stack Member list.
 - d. Click **Remove**.

You cannot remove a device from the stack while it is the segment reference device. If necessary, change the segment reference device to a different stacking device and then remove the stack member.

3. Disconnect the AOC or QSFP+ cables to remove the device that you do want from the stacking bus.
4. Disable Intrinsic HA Layer-2 Fallback on the stack.

**Note**

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 in conjunction with a TippingPoint technical support representative to restore the device to its original settings. [Learn more on page 6-1.](#)

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.

**Note**

You must have permission to manage a device in order to add the device to a stack.

If you are repurposing an existing device for use in the stack, always reset the device to factory settings, and then install the required TOS version. See [Learn more on page 6-1.](#)

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. [Learn more on page 4-8.](#)

To add a device to the stack

1. Use the SMS to place the stack in Intrinsic HA Layer-2 Fallback.
2. Install the AOC or QSFP+ cables to connect the new device to the stacking bus.
3. Manage the new stacking device with the SMS.

4. Add the stacking device to the stack.
 - a. In the SMS tools, click **Devices**.
 - b. In the **All Devices** workspace, double-click the stack.
 - c. In the **Summary** tab, click **Add**.
 - d. Select the device to add.
If the SMS cannot add the device to the stack, identify and resolve the issue.
 - e. Click **OK** and view the updated stack health.
 - f. If the device you are adding is intended to be the segment reference device, update the stack configuration to designate the device as the segment reference device.
5. Distribute the inspection profile to the stack.
6. Take the stack out of Intrinsic HA Layer-2 Fallback.

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.

Delete the stack

Delete the stack to return the devices to the SMS as standalone devices. 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 in conjunction with a TippingPoint technical support representative to restore the device to its original settings.

To delete the stack

Procedure

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

What to do next

After you delete the stack:

- Use the `debug factory-reset` command in conjunction with a TippingPoint technical support representative to restore the device to its original settings.
- Remanage each device on the SMS. Stacking is **disabled** on each device.
- Reconfigure inspection policies on the devices. Inspection policies are not preserved after the factory reset.
- Reconfigure profile distributions after you remanage the device on the SMS.

Granting permissions to the stack

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 3-8](#)
- [Grant the user group access to the stack on page 3-9](#)

Add stack management to the user role

Grant permission to a user role to manage a stack.

This capability requires the user group to also have access to the stack. [Learn more on page 3-9.](#)

To update the user role

Procedure

1. In the SMS tools, click **Admin**.

2. Click **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

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

Procedure

1. In the SMS tools, click **Admin**.
 2. Click **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.

Before you distribute a TOS update, enable Intrinsic HA Layer-2 Fallback on the stack. Intrinsic HA Layer-2 Fallback remains enabled until the stack primary confirms that there are enough devices in the stack with the same TOS version that are ready to inspect.

Distribute a TOS update to the stack using the same steps you would follow for a standalone TPS device.

Use the **Sync Health** tab to verify that the same TOS version is installed on each stacking device.

**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.

Differences between configuring a stack and a standalone device

The following information highlights options that are exclusive for configuring security policy on a stack:

- [Security policy configuration on page 3-10](#)
- [Events and reports on page 3-14](#)
- [System updates and snapshots on page 3-15](#)
- [SMS database restore to a different SMS on page 3-16](#)

Security policy configuration

Configure the security policy on the stack using the same steps you would follow for configuring the security policy for a standalone TippingPoint IPS or TPS security device.

Use the following guidelines when configuring the security policy for your stack.

TipingPoint Operating System (TOS) distribution

A TOS distribution to the stack places all of the stacking devices into Intrinsic HA Layer-2 Fallback while the TOS update is installed.

Perform a planned TOS update by enabling Intrinsic HA Layer-2 Fallback on the stack and then distributing the TOS update to the stack. Stacking requires the same TOS version on each of the stacking devices.

Digital Vaccine Labs package distribution

When you distribute a Digital Vaccine package to the stack, the SMS distributes Digital Vaccine, AUX DV, and DV Toolkit packages to each

member of the stack. All devices in a stack must have the same Digital Vaccine packages.


**Note**

Each time you add or delete a member in a stack, you must update the Digital Vaccine distribution schedule. This is because Digital Vaccines are always distributed according to which members were in the stack at the time the distribution was first scheduled. For example, if you schedule a distribution and then remove a device from the stack, the SMS still distributes the package to all the devices that were members of stack when the distribution was first scheduled, including the device you removed.

Inspection profile distribution

Distribute your inspection profiles so that they are sent to selected segments on the stack. To do this, specify the virtual segments or segment groups on the segment reference device when you distribute the profile. After you do this, the inspection profile goes to the corresponding segments or segment groups on each member of the stack.

Distribute an inspection profile to **all** segments of the stack, including any disabled ports.

If a network segment does not have a profile, a  Major indicator is displayed in the Sync Health tab.

Scheduled profile distribution

When working with scheduled profile distributions on the stack, consider the following points.

Scheduled profile distributions – Stack:

A scheduled profile distribution to the stack runs on the stack members that were in the stack when you created the scheduled profile distribution. If you reconfigure the stack, update the list of target devices in the scheduled profile distribution to include the current stack membership. For example, update the list of target devices when you:

- Add a device to the stack
- Remove a device from the stack
- Delete the stack

After you delete the stack, the scheduled profile distribution continues to run on the segment reference device.

Scheduled profile distributions – Segment Group:

A scheduled profile distribution to a segment group on the stack runs on the stack members that were in the stack when you created the scheduled profile distribution. If you reconfigure the stack, update the list of target devices in the scheduled profile distribution to include the current stack membership. For example, update the list of target devices when you:

- Add a device to the stack
- Remove a device from the stack
- Delete the stack

After you delete the stack, any scheduled profile distributions continue to run on all physical network segments that were in the stack. Scheduled profile distributions no longer run on a network segment without a physical network I/O module.

Device configuration

Configure the devices in the stack as you would a standalone device.

To edit the device configuration for the stack:

1. In the SMS tools, click **Devices**.
2. In the **All Devices** workspace, right-click the stack and select **Edit Stack Member Configuration**.
3. In **Device Configuration** options, configure the stacking devices.

Segment groups

When creating a segment group for the stack, choose from the physical segments on the segment reference device.

Virtual segment details - physical segments

When you create a virtual segment on the stack, the available physical segments consist of network segments.

Active Responder policy - quarantine actions

When you want a stack to quarantine network traffic, use the SMS to create an Active Responder policy that propagates the IPS Quarantine action set to the stack. Responder applies the policy thresholds to the stack so that a filter hit on any stack member is applied to the policy threshold, and any stack member that inspects the traffic can also quarantine the traffic when the stack-level policy is triggered.

Inspection bypass rules

When working with inspection bypass rules, consider the following points:

- Create inspection bypass rules on the segment reference device.
- Network I/O slots are available for inspection bypass rules.
- Inspection Bypass mismatches are displayed in the **Sync Health** tab.

To resolve any issues, update the inspection bypass rules on the segment reference device. The Sync Health tab automatically updates the synchronization status.

- The SMS synchronizes inspection bypass rules across the stack when you finish updating inspection bypass rules on the segment reference device.



Note

Before you configure an inspection bypass rule, distribute an inspection profile to the corresponding segments.

VLAN translation

When working with VLAN translation, consider the following points:

- Network I/O slots are available for VLAN translation.
- Create VLAN translations on the physical segments that connect to the network. If the same network is on more than one segment, create the same VLAN translations on the segments. VLAN translation occurs after inspection but before the traffic exits the stack, so it is important to only configure VLAN translation on the segments that connect to the network.

Events and reports

View events and reports for a stack using the same steps you would follow for a standalone TippingPoint IPS or TPS security device.

The following table provides stacking-related information for events and reports.

FOR	CONSIDER THESE POINTS
Events	<p>When you create an inspection query with filter criteria for the stack, consider the following points:</p> <ul style="list-style-type: none">• Query the segments from the segment reference device to include events from all corresponding segments across the stack.• You can filter inspection events by stack. In the Device/Segment/Rule section of the criteria, there is a box for selection of Device/Group/Stack. An inspection event indicates the stack member that inspected the flow.• A saved event query on the segment reference device includes events from any devices that were stack members when you created the query. If you replace the segment reference device, update your event query to include any stack members.

FOR	CONSIDER THESE POINTS
Reports	<p>When you report on the stack, consider the following points:</p> <ul style="list-style-type: none"> • Query a segment from the segment reference device to include data from all corresponding segments across the stack. • Stack member-level reporting shows the traffic statistics for the specified segment. • Saved report queries on the segment reference device include data from any devices that were stack members when you created the query. If you replace the segment reference device, update your report query to include any stack members. • Run the Device Traffic report on the stack or on a particular segment of the segment reference device to report on statistical changes in network traffic patterns across the stack. Traffic reports include traffic information from network I/O slots only.

System updates and snapshots

Do not rollback to an unsupported TOS version or to a snapshot that was taken of the device before it was added to the stack.

If you rollback to a snapshot that has a different stack resiliency setting, the **Sync Health** tab in the SMS displays the misconfiguration. To resolve this issue, edit and save the stack configuration with the stack resiliency setting you want.

Never rollback to an unsupported version. For example, if you rollback the TippingPoint Operating System on a stacking device from v3.9.0 to v3.8.x, then the unsupported TOS version prevents the device from participating in the stack. This problem can also occur if you restore a snapshot on a stack member, but the snapshot was taken before the device was added to the stack.



Note

If you restore a stacked device snapshot to a standalone device, the device state will be invalid. As a workaround, use the `reboot -full` command to put the device back into a valid state.

SMS database restore to a different SMS

When you restore the SMS backup to a different SMS, and the SMS manages a stack with virtual segments, you must manually repair the stack configuration to update its virtual segments.

To repair the stack configuration

1. Click **Devices** on the SMS toolbar.
2. In the **All Devices** workspace, add each of the devices in the stack.
3. In the left navigation pane, click **Virtual Segments**.
4. In the Virtual Segments list, edit and save (without making any changes) each virtual segment in the stack with a physical segment (including any hidden segments). A *hidden segment* is a segment on a stacking device that does not have a network I/O module.



Note

Use the **Segments Assigned** column to identify the virtual segments with physical segments and hidden segments. For example, a virtual segment with a Segments Assigned value of 8 (16 hidden) indicates there are eight physical segments and 16 hidden segments.

5. Delete any virtual segments that have no physical or hidden segments. For example, delete a virtual segment where the Segments Assigned value is 0 (0 hidden).

Chapter 4

Troubleshooting

Use the following information to identify and resolve stacking issues:

- *Verify AOC cable installation on page 4-2*
- *View stacking status on page 4-3*
- *Verify stack health and synchronization on page 4-7*
- *Resolve issues adding a device to the stack configuration on page 4-28*
- *View stacking tier statistics on page 4-28*
- *Intrinsic HA Layer-2 Fallback on page 4-30*
- *Export a Tech Support Report on page 4-33*
- *CLI commands for stacking on page 4-34*

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.

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



The next example shows a special purpose port with the AOC cable partially inserted upside down.



View stacking status

Use the **Devices** workspace to view and manage the stack and its devices.

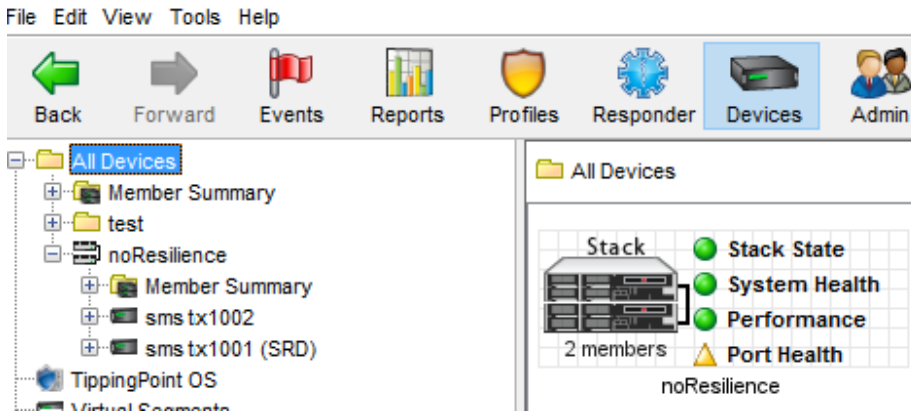
Device details

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.

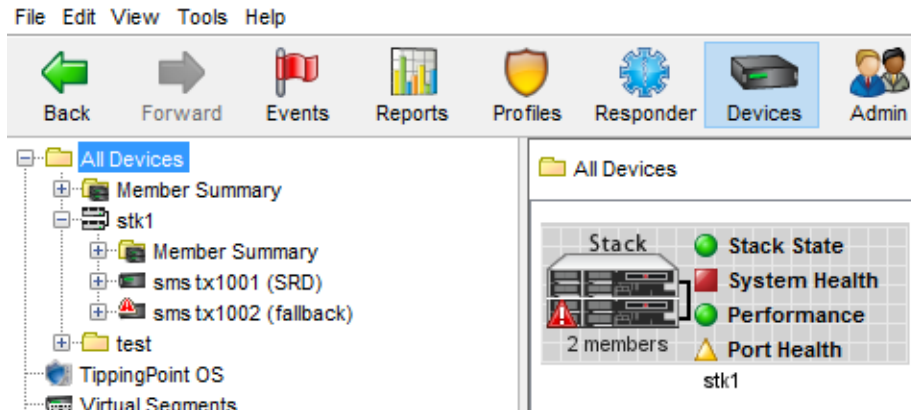
Stack is normal

The stack state is normal.




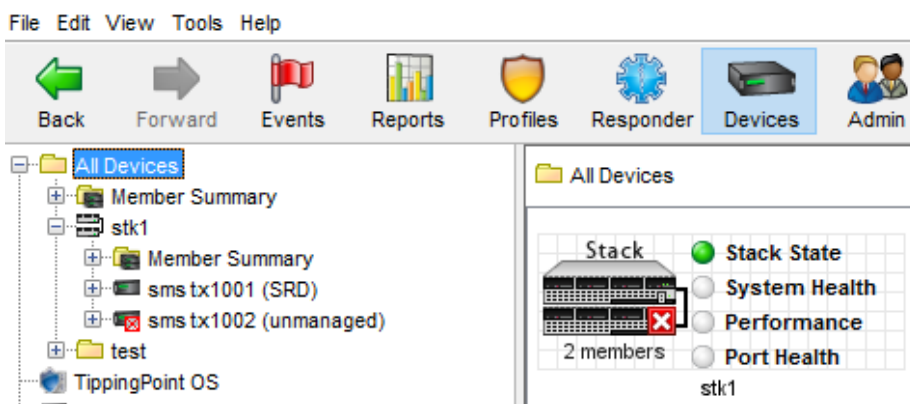
Stack with a device in Intrinsic HA Layer-2 Fallback

The following icon indicates that a device is in Intrinsic HA Layer-2 Fallback:





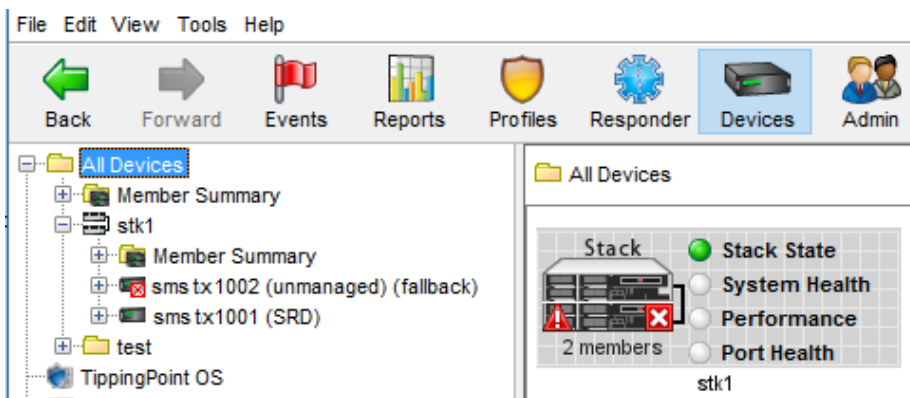
Stack with an unmanaged device

The  icon indicates that the **smstx1002** device is unmanaged by the SMS and another device could be in Intrinsic HA Layer-2 Fallback. The navigation pane indicates that the **smstx1001** device is the segment reference device for the stack.




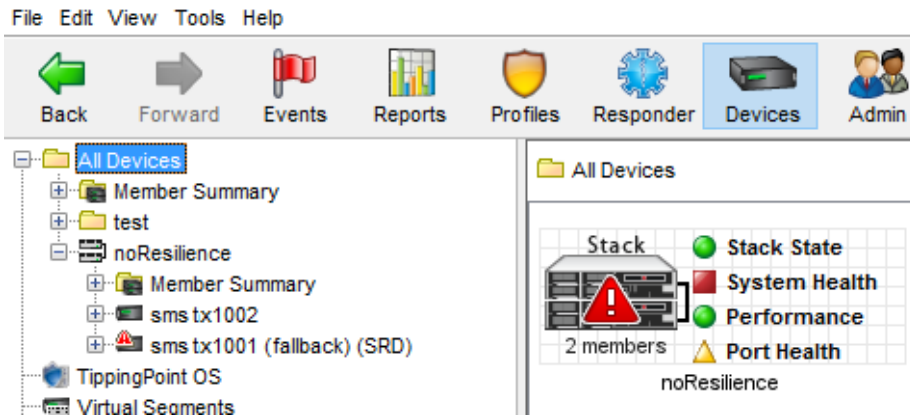
Stack with an unmanaged device that is also in Intrinsic HA Layer-2 Fallback

The  icon and the  icon indicate that a device is not managed by the SMS and another can be in Intrinsic HA Layer-2 Fallback.



Stack is in Intrinsic HA Layer-2 Fallback

The  icon indicates the stack is in Intrinsic HA Layer-2 Fallback.

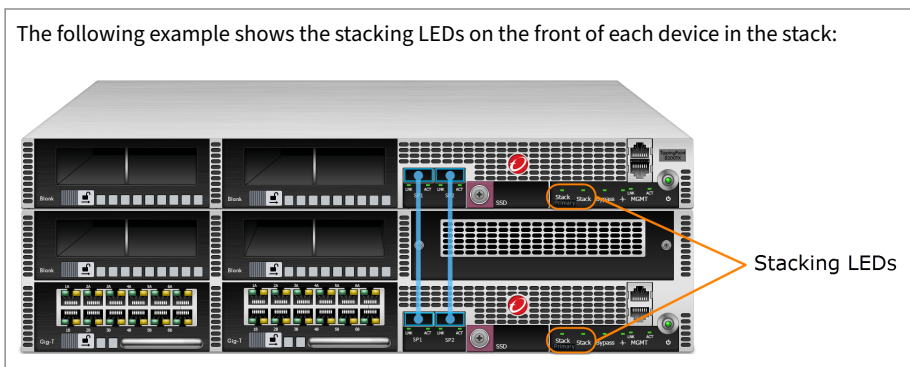


Front panel stacking LEDs

Use the front panel stacking LEDs to identify the stacking status directly from the device:

- **Stack:** Indicates whether stacking is enabled on the device. Stacking is automatically enabled when you add the device to the stack configuration. If necessary, remove the device from the stack configuration and then add it again to enable stacking. LED color indicates the following states:
 - **Solid green:** Indicates that the device is ready to inspect and is inspecting network traffic.
 - **Off:** Indicates that stacking is not enabled on the device.
- **Stack Primary:** Indicates whether the device is the stack primary. The **stack primary** is a device role that is responsible for managing stack configuration and states. The devices in the stack automatically elect the stack primary. All stack members are eligible for election to stack primary.
 - **Solid green:** Indicates that the device is the stack primary.
 - **Off:** Indicates that the device is not the stack primary.

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



Device shelf-level graphic

The device shelf-level graphic, as shown in the following example, identifies the stacking status:

- The **STK** LED indicates whether stacking is enabled. If the **STK** LED is green, stacking is enabled.



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.

Perform stack health troubleshooting steps in the following order:

1. [View overall health of the stack on page 4-8](#)
 2. [Verify stacking bus state on page 4-11](#)
 3. [Verify stack member state on page 4-14](#)
 4. [Verify device state on page 4-15](#)
- Use the **Sync Health** tab to verify the synchronization status of each device in the stack. If synchronization is in a degraded state, use the Issues table to troubleshoot and resolve any issues. [Learn more on page 4-17](#).

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






Procedure






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 special purpose port status information and suggested actions.


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 Layer-2 Fallback.	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 Layer-2 Fallback.	Disable Intrinsic HA Layer-2 Fallback on the stack.

STATUS	INFORMATION	SUGGESTED ACTION
 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 <code>Run Level 12</code> in the boot sequence. If necessary, reboot the device.
	Indicates that the number of devices in the stacking bus does not match the 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 Layer-2 Fallback but can return to  Ready to Inspect - Normal when the stack primary 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 primary returns the stack to  Ready to Inspect - Normal. Learn more on page 3-3.

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

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

STATUS	INFORMATION	SUGGESTED ACTION
 Connected in a ring	Indicates that the AOC or QSFP+ cables are installed correctly.	No action is required.

STATUS	INFORMATION	SUGGESTED ACTION
 Not Connected in a ring	Indicates that the AOC or QSFP+ cables are not installed correctly.	Verify the stacking bus health.

- **Stack Resilience** — Indicates whether the stack goes into Intrinsic HA Layer-2 Fallback if a single device is not ready to inspect. [Learn more on page 4-30.](#)
- **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 TPS devices in the stack configuration and does not reflect the number of devices in the stacking bus.

**Note**

For information about the status of the stacking bus topology, use the **Stack Port A** and **Stack Port B** columns. [Learn more on page 4-11.](#)

Verify stacking bus state



The **Summary** tab displays stacking bus health by checking the state of the special purpose 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

Procedure

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 special purpose port connectivity:

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

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 to the stack to enable stacking. 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 special purpose port connectivity.


The following information provides special purpose port status information and suggested actions.

STATUS	INFORMATION	SUGGESTED ACTION
 <i>devicename</i>	Indicates the device to which the special purpose port is resolved.	No action is required.
 <No Peer>	Indicates a peer device is not connected to the special purpose port.	Validate that the special purpose port is connected to a special purpose port on a peer device.
	Indicates stacking is not enabled on the peer device.	Validate that stacking is enabled on the peer device.
 <Unknown> (<i>mac-address-hex</i>)	Indicates the peer device is not managed by the SMS.	Manage the peer device with the SMS.
 No peer information is available	Indicates the peer device has not returned any stacking information.	Verify that the special purpose port connects the peer device 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.

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 special purpose port.	Validate that the special purpose port is connected to a peer device.
	Indicates the peer device that is connected to the special purpose 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 special purpose port references a device that is not actually a part of the stack. This message appears once for each special purpose port.	Update the stack configuration to add the device.
 Not in stack	Indicates that the device is not in the stack topology.	Validate that the SP port connects to a special purpose port on a peer device.
 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.

STATUS	INFORMATION	SUGGESTED ACTION
 Unknown peer(s) found	The peer device that is connected to the special purpose port is not managed by the SMS.	Manage the peer device with the SMS.
	The peer device is not added to the SMS stack configuration.	Use the SMS to update the stack configuration.

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

Procedure

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.

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.

STATUS	INFORMATION	SUGGESTED ACTION
 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 Layer-2 Fallback.	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 Layer-2 Fallback.	Disable Intrinsic HA Layer-2 Fallback on the stack.
 RTI - L2FB	Indicates that the stack member is in Intrinsic HA Layer-2 Fallback but can return to  Ready to Inspect - Normal when the stack primary determines that the minimum number of devices are ready to inspect.	Depending on whether the stack is a resilient configuration, all but one of the stack members, or all of the stack members must declare they are  Ready to Inspect - Normal before the stack primary returns the stack to  Ready to Inspect - Normal. Learn more on page 3-3.

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

Procedure

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.

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.	Use the SMS to manage the device.
 Not Communicating	Indicates that the device is not communicating across the management network with the SMS.	Verify network connectivity between the SMS and the device. Also, verify the required ports are not blocked.
 Layer 2 Fallback	Indicates that the device is not inspecting traffic because Intrinsic HA Layer-2 Fallback is enabled.	If you enabled Intrinsic HA Layer-2 Fallback on the device, disable Intrinsic HA Layer-2 Fallback. If you cannot disable Intrinsic HA Layer-2 Fallback, determine whether stacking has put the device into Intrinsic HA Layer-2 Fallback.
 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 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, such as virtual segments and profiles. If they do not match, the SMS indicates the mismatch and shows the degraded stack health.





To verify stack synchronization



Procedure





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.





STACK INFORMATION	INFORMATION	SUGGESTED ACTION
 TOS	Indicates the TOS version for each of the devices. Critical indicator  : Indicates a mismatch in versions or distribution. Tip: To filter synchronization information by this type of issue, use the Type column to filter by TOS Versions.	Distribute the TOS version to the stack.







STACK INFORMATION	INFORMATION	SUGGESTED ACTION
 Digital Vaccine	<p>Indicates the Digital Vaccine version for each of the devices.</p> <p>Major indicator :</p> <p>Indicates a 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 Digital Vaccine package to the stack.</p>
 <i>{aux-dv-sub type-name}</i> ThreatDV Versions	<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 :</p> <p>Indicates a 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>





STACK INFORMATION	INFORMATION	SUGGESTED ACTION
 {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 : Indicates a mismatch in distributions (not versions).</p> <p>If the DVT is not displayed, the DVT was not distributed to any devices.</p> <p>Tip: To filter synchronization information by this type of issue, use the Type column to filter by DVToolkit Versions.</p>	Distribute the DVToolkit package to the stack.



STACK INFORMATION	INFORMATION	SUGGESTED ACTION
<p> {physical-segment-name-and-direction}</p>	<p>Indicates the  {profile name} {profile-version} was distributed to a physical segment on each of the devices.</p> <p>Major indicator : Mismatch between profile name, profile version, or distribution.</p> <p>Major indicator : <Unknown> Indicates 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 physical segment.</p>



STACK INFORMATION	INFORMATION	SUGGESTED ACTION
 {virtual-segment-name}	<p>Indicates the  {profile-name} {profile-version} was distributed to a virtual segment on each of the devices.</p> <p>Major indicator  : <Unknown> Indicates 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  : Indicates a mismatch between profile name, profile version, or distribution. There is one row for each virtual segment.</p> <p>Tip: To filter synchronization information by this type of issue, use the Type column to filter by Virtual Segment's Profiles.</p>	Distribute the profile to the virtual segment.




STACK INFORMATION	INFORMATION	SUGGESTED ACTION
 Missing {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>
 Extra {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 the Type column to filter by Extra Virtual Segment.</p>	<p>Delete the extra virtual segment if it is not applicable. Or, edit and save the virtual segment to update the stack.</p>

STACK INFORMATION	INFORMATION	SUGGESTED ACTION
<p> Mismatched group for <i>{virtual-segment-name}</i></p>	<p>Indicates the  <i>{segment-group-name}</i> to which a virtual segment belongs for each of the devices.</p> <p>Critical indicator : 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> Mismatched group for <i>{physical-segment-name}</i></p>	<p>Indicates the  <i>{segment-group-name}</i> to which a physical segment belongs for each of the devices.</p> <p>Critical indicator : The mismatch is listed.</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>

STACK INFORMATION	INFORMATION	SUGGESTED ACTION
 Extra rule <i>{inspection-bypass-rule-name}</i>	<p>Indicates that there is an inspection bypass rule on a stacking device that is not on the segment reference device.</p> <p>Critical indicator : There is one row for each inspection bypass rule.</p> <p>Tip: To filter synchronization information by this type of issue, use the Type column to filter by Extra Rule.</p>	Edit and save the inspection bypass rule (without making any changes) to update the stack.
 Missing <i>{inspection-bypass-rule-name}</i>	<p>Indicates that there is an inspection bypass rule on the segment reference device that is missing from a device in the stack.</p> <p>Critical indicator : There is one row for each inspection bypass rule.</p> <p>Tip: To filter synchronization information by this type of issue, use the Type column to filter by Missing Rule.</p>	Edit and save the inspection bypass rule (without making any changes) to update the stack.






STACK INFORMATION	INFORMATION	SUGGESTED ACTION
Stack Resilience <i>{stack-resilience-value}</i>	<p>Indicates that there is at least one device with a different Stack Resilience option than what is configured for the stack. Critical indicator : The mismatch is listed.</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.
 SSL Enabled	Indicates that SSL inspection is enabled on some of the devices in the stack but not all of them.	Edit the device configuration on each stacking device to verify that SSL inspection is enabled (Devices > All Devices > device-name > Device Configuration).

STACK INFORMATION	INFORMATION	SUGGESTED ACTION
 SSL Licensed	Indicates that some of your devices have a license that allows SSL inspection and others that do not allow SSL inspection.	<p>Update your license package to assign a product capability that you have purchased, such as SSL inspection, to each stacking device. When you install the license package on the device, be sure to reboot the device and enable the license capability for SSL inspection.</p> <hr/> <p> Important</p> <p>Do not reboot all devices in a stack at the same time. When you have to reboot devices in a stack configuration, reboot each device that you updated sequentially. Allow each device to finish the boot sequence completely—ensuring that the SMS has successfully managed the device—before rebooting the next device.</p> <hr/> <p>Go to TMC at https://tmc.tippingpoint.com/ to review and manage the capabilities in your license package.</p>

STACK INFORMATION	INFORMATION	SUGGESTED ACTION
 License Throughput	<p>Indicates that some of your devices have a license for a different inspection throughput rate than the other devices.</p>	<p>Update your license package to assign a product capability that you have purchased, such as inspection throughput, to a particular security device.</p> <p>Go to TMC at https://tmc.tippingpoint.com/ to review and manage the capabilities in your license package.</p>
 Extra VLAN {translation-description}	<p>Indicates that there is a VLAN translation rule on a stacking device that is not on the segment reference device.</p> <p>There is one row for each VLAN translation rule.</p> <p>Tip: To filter synchronization information by this type of issue, use the Type column to filter by Extra VLAN.</p>	<p>Remove the device from the stack, restore the device to its original settings, and then add the device to the stack.</p> <p>If necessary, edit the VLAN translation mappings for the segment reference device to include the VLAN translation mapping from the stacking device.</p>
 Missing VLAN {translation-description}	<p>Indicates that there is a VLAN translation on the segment reference device that is missing from a device in the stack.</p> <p>There is one row for each VLAN translation rule.</p> <p>Tip: To filter synchronization information by this type of issue, use the Type column to filter by Missing VLAN.</p>	<p>Edit and save the VLAN translation mapping on the segment reference device (without making any changes) to update all of the stacking devices.</p>

Resolve issues adding a device to the stack configuration

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

STATUS	INFORMATION	SUGGESTED ACTION
 Ready for stacking	Indicates that there is no issue with adding the device to the stack.	No action is required.
 This device's TOS version doesn't match the TOS version for the selected devices.	Indicates that there is a TOS version mismatch.	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.
 This device does not support stack sizes of more than ## devices.	Indicates a device is valid for stacking, but that the maximum number of devices in the stack has been reached.	Remove a device from the stack so that you can add the device.
 Device is not communicating	Indicates that the device is not communicating with the SMS.	Verify network connectivity between the SMS and the device. Also, verify the required ports are not being blocked.
 Device is unmanaged	Indicates that the SMS no longer manages the device.	Use the SMS to manage the device.

View stacking tier statistics

Use the SMS to view tier statistics on the device for stacking (Tier S) in addition to tiers 1–4.

The tier statistics area provides information on packets and speed as measured in Mbps by tier. Refer to the *SMS User Guide* for more information about tier statistics for the various TippingPoint devices.

Tier S data includes stacking data from the special purpose ports.

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 Layer-2 Fallback, 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 that is inspected by this device as a ratio of the segment Rx traffic.

INSPECTION TIER	INFORMATION
Stack : Stack Ports	<p>This inspection tier presents special purpose 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"> • <code>Stack Rx Mbps</code> displays the aggregate traffic that is received on both special purpose ports. • <code>Stack Tx Mbps</code> displays the aggregate traffic that is transmitted from both special purpose ports. • <code>Stack Rx > Stack Tx</code> displays the total amount of transit or through traffic on the special purpose ports; for example, traffic that is received on special purpose port 1, which is forwarded by the switch to special purpose port 2. • <code>Stack Rx > Seg Tx</code> displays the amount of return traffic coming in on a special purpose port that is returning to the outbound network segment. • <code>Stack ratio to tier 1</code> displays the percentage of traffic that is inspected by this device as a ratio of the stack Rx traffic.

Intrinsic HA 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 either permits or blocks all traffic on each segment, depending on the Intrinsic HA action setting for the segment. Any permitted traffic is not inspected.

You can enable Intrinsic HA Layer-2 Fallback on a stack member or the entire stack, for example, to perform scheduled maintenance. When you finish, disable Intrinsic HA Layer-2 Fallback to resume normal operation.

Stacking automatically enables and disables Intrinsic HA Layer-2 Fallback 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 ready to inspect, the stack primary takes the stack out of Intrinsic HA Layer-2 Fallback. [Learn more on page 3-3.](#)

- **Not Ready to Inspect (NRTI)** indicates that a device or the stack is not ready to inspect traffic.

When a device or stack is not ready to inspect, Intrinsic HA Layer-2 Fallback remains enabled until the cause is resolved. In some cases, this is a temporary recoverable condition and in other cases, recovery requires manual intervention. [Learn more on page 4-14.](#)

**Tip**

If a device or the stack is in Intrinsic HA Layer-2 Fallback, disable Intrinsic HA Layer-2 Fallback on the stack to restore the stack to normal operation. If the stack does not return to normal operation, verify the stack health to determine why the stack is in Intrinsic HA Layer-2 Fallback and resolve any issues. [Learn more on page 4-7.](#)

Enable Layer-2 Fallback on the stack

Enable Intrinsic HA Layer-2 Fallback on the stack to either permit or block all traffic on each segment of any devices in the stack, depending on the Intrinsic HA action setting for each segment. When you disable Layer-2 Fallback on the stack, the stack returns to normal operation.

To resume normal operation, the stack must validate:

- The minimum number of devices are ready to inspect. [Learn more on page 4-7.](#)
- The stack members communicate regularly with the stack primary. 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 not ready to inspect.
- The same TOS version is installed on each device. [Learn more on page 4-17.](#)

If you manually enable Layer-2 Fallback on the stack, you must also disable it to resume normal operation. If necessary, resolve any Layer-2 Fallback issues on a stacking device so that you disable Layer-2 Fallback.

To configure Layer-2 Fallback on the stack

Procedure

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** – Enables Layer-2 Fallback.
 - **Normal** – Disables Layer-2 Fallback.
-

Enable Layer-2 Fallback on a stacking device

Enable Intrinsic HA Layer-2 Fallback on a stacking device to either permit or block all traffic on any segment, depending on the Intrinsic HA action setting for each segment.

When you disable Layer-2 Fallback on a stacking device, the stack primary determines whether to return the device and the stack to normal operation. [Learn more on page 4-30.](#)

Before you enable Layer-2 Fallback on a stacking device, consider whether the loss of the device would place the entire stack into Layer-2 Fallback. For example:

- Resilient stack configuration – The loss of a single device would not place the stack into Layer-2 Fallback.
- Single network segment device – The loss of the network segment device would place the stack into Layer-2 Fallback.

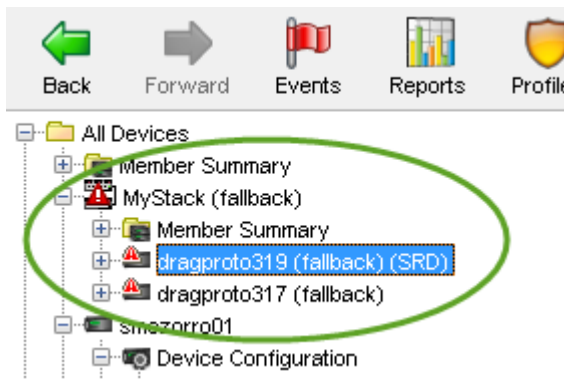
To configure Layer-2 Fallback on a stacking device

Procedure

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 Layer-2 Fallback, the name of the device is appended by **(fallback)**. In the following example, **MyStack** and its stack members are in Layer-2 Fallback.



4. Click the device that is in Layer-2 Fallback.
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** – Enables Layer-2 Fallback.
 - **Normal** – Disables Layer-2 Fallback.

Export a Tech Support Report

You can collect diagnostic information from a TPS device by exporting a Tech Support Report (TSR). The TSR collects information from diagnostic commands and log files into a report that customer support can use to diagnose issues with the device.

**Tip**

When you export a TSR from the SMS, the TSR does not include snapshot information. However, you can create a snapshot from the SMS.

To collect diagnostic information for the stack

1. Use the SMS to export a TSR from each device in the stack.
2. Save each TSR to your local system.
3. Email the TSR files to customer support for assistance.

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 or TPS device and select **Export TSR**.
 - 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

From the device CLI, run the **show stacking** command to display stacking status information. For more information about stacking-related commands, see the *TPS Command Line Interface Reference*.

Chapter 5

Considerations

Consider these points when planning your stacking deployment:

- 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.
 - 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 device CLI.
- All stack members must use consistent sets of inspection profiles to ensure inspection policies are applied consistently, regardless of which device inspects the traffic.



Note

There are differences between configuring a stack of devices compared with configuring a standalone device. [Learn more on page 3-10.](#)

Chapter 6

Repurposing a device

If you have an existing TPS device that is not currently deployed in your network, you can repurpose the device 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.

To repurpose a device, use the `debug factory-reset` command to restore the device to its original settings.

Consider the following points when you repurpose a device for use in a stack:

- Install the same TippingPoint Operating System (TOS) version on each device in the stack.
- Configure the same slot on each device with either the **same** network I/O module or **no** network I/O module as compared to the network segment device.



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: TPEM09848/230927