5.0.0 TippingPoint™ Threat Protection System
TX Series Stacking Deployment Guide
Actionable threat defense against known and zero-day attacks
# 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 ....................................................................................................... 8

Multiple network segment device configuration .......................................................................... 9

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

Grant permissions to the stack ............................................................................................... 16

Add stack management to the user role ................................................................................. 16
Grant the user group access to the stack ................................................................. 17
Distribute a TOS update ............................................................................................. 17

**Troubleshooting** ..................................................................................................... 18

Verify AOC cable installation .................................................................................... 18
Verify stacking status .................................................................................................... 19
Device details ................................................................................................................ 19
Front panel stacking LEDs .......................................................................................... 22
Device shelf-level graphic ............................................................................................ 23

Verify stack health and synchronization ..................................................................... 23
View overall health of the stack .................................................................................. 24
Verify stacking bus state .............................................................................................. 26
Verify stack member state ........................................................................................... 29
Verify device state ......................................................................................................... 30
Verify stack synchronization ......................................................................................... 32

Resolve issues adding a device to the stack ............................................................... 40
View stacking tier statistics ......................................................................................... 41

Enable or disable Intrinsic High Availability Layer-2 Fallback ..................................... 43
Enable or disable Intrinsic HA L2FB on the stack ....................................................... 43
Enable or disable Intrinsic HA L2FB on a stacking device .......................................... 44

Export a Tech Support Report ...................................................................................... 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
SP port......................................................................................................................................52
stack master..............................................................................................................................52
stack resiliency..........................................................................................................................52
stacking..................................................................................................................................... 52
stacking bus..............................................................................................................................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 TX Series Threat Protection System (TPS) 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 Threat Protection System (TPS) by grouping multiple TX Series devices and pooling their resources.

You can configure up to five TX Series devices in a stack. The stack operates as a single device that you manage on the TippingPoint Security Management System (SMS). The devices in the stack can be all 8200TX or 8400TX TPS devices, or a mix of both 8400TX and 8200TX security devices. 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.

The following TippingPoint software is supported for stacking:

- **TippingPoint SMS v5.0.0, or later** - Centrally manages each stack of devices.
- **TippingPoint Operating System (TOS) v5.0.0, or later** - Must be installed on each security device.

**Note:** No additional licensing is required to implement stacking.

Not all TippingPoint TX Series TPS 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 8.

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 8200TX or 8400TX device.

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

8200TX

8400TX
**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**

A TX Series device stack consists of two or more devices. The *stacking bus* consists of a pair of SP ports on each stacking device that connect each device to its peer in a ring topology.

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.

**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.

**To install the stacking components**

1. Install the network I/O modules on the network segment device so that you can connect the device to the network.
   
   For information about how to install I/O modules, see the *TX Series Hardware Installation and Safety Guide*.

2. Install the AOC 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 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 18 for more information.

**Examples with the AOC cables installed**
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.

**Figure 1. TippingPoint TX Series TPS – the AOC cables are installed properly**

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

**Figure 2. TippingPoint TX Series TPS – stack with network I/O modules installed in slots 1 and 2**

**Create the stack in the SMS**

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

The process is:

1. Add the stacking devices to the SMS
2. Create the stack
3. Distribute the inspection profile
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, v5.0.0 or later. The TOS version must be the same on each TX 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.
4. Choose **Normal** for the Stack Resilience option.

   For information about the **N+1 Redundancy** option, see *Resilient stack configuration* on page 8.

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 a TX Series (8200TX or 8400TX) TPS.

   - 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 23.
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 32.

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**

![Profile Distribution Example](image)

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 9.

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 TX Series TPS – resilient stack configuration](image)

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

**Figure 6. TippingPoint TX Series TPS – network I/O slot numbers**

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 7. TippingPoint TX Series TPS – 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
- Grant permissions to the stack on page 16
- Distribute a TOS update on page 17

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 8.

**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 stack resiliency on page 12.
   - **Normal** – This option automatically places the stack and all of its devices 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.

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 43.
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.
   
   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 43.

## 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 43.

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 43.

### 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.

   **Note:** You cannot remove a device from the stack while it is the SRD. If necessary, change the SRD to a different stacking device and then remove the device from the stack.

5. Click OK.

   The stack health is updated. See Verify stack health and synchronization on page 23.
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 24.

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 43.
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 43.

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 16.

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 23.

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. See *Distribute the inspection profile* on page 8.

**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.

**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 16
- **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.
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 43.

Distribute a TOS update to the stack using the same steps you would follow for a standalone TippingPoint TX Series TPS. 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 32.

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 18
- View stacking status on page 19
- Verify stack health and synchronization on page 23
- Resolve issues adding a device to the stack on page 40
- View stacking tier statistics on page 41
- Enable or disable Intrinsic High Availability Layer-2 Fallback on page 43
- Export a Tech Support Report on page 45
- CLI commands for stacking on page 46

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 an SP port with the AOC cable installed

The following example shows an SP port with the AOC cable installed correctly.

Figure 8. TippingPoint TX Series TPS – SP port with the AOC cable installed correctly
The next example shows an SP port with the AOC cable installed incorrectly.

**Figure 9. TippingPoint TX Series TPS – SP port with the AOC cable partially inserted upside down**

---

**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 \texttt{smstx1002} device is unmanaged by the SMS and another device could be in Intrinsic HA L2FB. The navigation pane indicates that the \texttt{smstx1001} device is the segment reference device (SRD) for the stack.

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

The \texttt{A} icon and the \texttt{X} 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**: Indicates whether 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:
  - **Solid green**: Indicates that the device is RTI and is inspecting network traffic.
  - **Off**: Indicates that stacking is not enabled on the device.

- **Stack Master**: Indicates whether the device is the stack master. The stack master is automatically elected by the devices in the stack. All stack members are eligible for election to stack master.
  - **Solid green**: Indicates that the device is the stack master.
  - **Off**: Indicates that the device is not the stack master.

The following example shows the stacking LEDs on the front of each device in the stack:
Device shelf-level graphic

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

- 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.

  (Best Practice) Perform stack health troubleshooting steps in the following order:
  a. **View overall health of the stack** on page 24
  b. **Verify stacking bus state** on page 26
  c. **Verify stack member state** on page 29
  d. **Verify device state** on page 30
• 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 32.

**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 SP port status information and suggested actions.

<table>
<thead>
<tr>
<th>Table 1. SP port status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
</tr>
<tr>
<td>---------------------------</td>
</tr>
<tr>
<td>![Ready to Inspect - Normal]</td>
</tr>
<tr>
<td>![Not Ready to Inspect - Unknown]</td>
</tr>
<tr>
<td>![Not Ready to Inspect - Rebooting]</td>
</tr>
<tr>
<td>Status</td>
</tr>
<tr>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Not Ready to Inspect - Layer 2 Fallback</td>
</tr>
<tr>
<td>Not Ready to Inspect - Recoverable Layer 2 Fallback</td>
</tr>
<tr>
<td>Not Ready to Inspect - Invalid</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Ready to Inspect - Layer 2 Fallback</td>
</tr>
</tbody>
</table>
- **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

<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>![green_circle] Connected in a ring</td>
<td>Indicates that the AOC cables are installed correctly.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>![red_square] Not Connected in a ring</td>
<td>Indicates that the AOC cables are not installed correctly.</td>
<td>Verify the stacking bus health. See <em>Verify stacking bus state</em> on page 26. See also, <em>Install the stacking components</em> on page 4.</td>
</tr>
</tbody>
</table>

- **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 26.

### Verify stacking bus state

The **Summary** tab displays stacking bus health by checking the state of the SP 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 SP 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 SP port connectivity. See also, *Device shelf-level graphic* on page 23.

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

<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td>![devicename]</td>
<td>Indicates the device to which the SP port is resolved.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>![&lt;No Peer&gt;]</td>
<td>Indicates a peer device is not connected to the SP port.</td>
<td>Validate that the SP port is connected to a SP port on a peer device. See <em>Install the stacking components</em> on page 4.</td>
</tr>
<tr>
<td></td>
<td>Indicates the peer device that is connected to the SP port does not have stacking enabled.</td>
<td>Validate that stacking is enabled on the peer device. See <em>View overall health of the stack</em> on page 24.</td>
</tr>
<tr>
<td>![&lt;Unknown&gt; (mac-address-hex)]</td>
<td>Indicates the peer device that is connected to the SP port is not managed by the SMS.</td>
<td>Add the peer device to the SMS. See <em>Add the stacking devices to the SMS</em> on page 6.</td>
</tr>
<tr>
<td>![No peer information is available]</td>
<td>Indicates no stacking information was returned from a peer device.</td>
<td>Verify that the SP port is connected to the same stacking bus as the segment reference device.</td>
</tr>
</tbody>
</table>

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

The following information provides stack topology status information and suggested actions.
<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segment Reference</td>
<td>Indicates that the device has been designated as the segment reference device and is ready for stacking.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Normal</td>
<td>Indicates that the device is functioning normally.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>Missing peer</td>
<td>Indicates a peer device is not connected to the SP port.</td>
<td>Validate that the SP port is connected to a peer device. See <em>Install the stacking components</em> on page 4.</td>
</tr>
<tr>
<td></td>
<td>Indicates the peer device that is connected to the SP port does not have stacking enabled.</td>
<td>Validate that stacking is enabled on the peer device.</td>
</tr>
<tr>
<td>Peer {device-name} is not a stack member</td>
<td>Indicates that a device SP port references a device that is not actually a part of the stack. This message appears once for each SP port.</td>
<td>Update the stack configuration to add the device. See <em>Add a device to the stack</em> on page 15.</td>
</tr>
<tr>
<td>Not in stack</td>
<td>Indicates that the device is not in the stack topology.</td>
<td>Validate that the SP port is connected to a peer device that is a member of the stack. See <em>Install the stacking components</em> on page 4.</td>
</tr>
<tr>
<td>Wrong I/O Modules in slot(s) {slot numbers}</td>
<td>Indicates that there is an I/O module on the device that does not match the I/O module in the segment reference device.</td>
<td>Verify that the slot on the device is configured with the same network I/O module or no network I/O module</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RTI - Normal</strong></td>
<td>Indicates that the stack member is working correctly.</td>
<td>No action is required.</td>
</tr>
<tr>
<td><strong>NRTI - Unknown</strong></td>
<td>Indicates that the stack member is not inspecting traffic for an unknown reason.</td>
<td>This is a transitory state and no action is required.</td>
</tr>
<tr>
<td><strong>NRTI - Rebooting</strong></td>
<td>Indicates that the stack member is not inspecting traffic because it is rebooting.</td>
<td>This is a transitory state and no action is required.</td>
</tr>
</tbody>
</table>
### 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

<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Normal]</td>
<td>Indicates that the device is working normally.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>![Updating]</td>
<td>Indicates that the device is updating its status.</td>
<td>This is a transitory state and no action is required.</td>
</tr>
<tr>
<td>![Unmanaged]</td>
<td>Indicates the device is not managed by the SMS.</td>
<td>In the SMS, manage the device:</td>
</tr>
<tr>
<td>![Not Communicating]</td>
<td>Indicates that the device is not communicating across the management network with the SMS.</td>
<td>Verify network connectivity between the SMS and the device. Also, verify the required ports are not blocked. For more information, see the Security Management System User Guide.</td>
</tr>
<tr>
<td>![Layer 2 Fallback]</td>
<td>Indicates that the device is not inspecting traffic because Intrinsic HA L2FB is enabled.</td>
<td>If you enabled Intrinsic HA L2FB on the device, disable Intrinsic HA L2FB. See Intrinsic HA on page 44. 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 29.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Stack information</th>
<th>Information</th>
<th>Suggested Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢 TOS</td>
<td>Indicates the TippingPoint Operating System (TOS) version for each of the devices. Critical indicator 🟢 Mismatch in versions or distribution.</td>
<td>Distribute the TOS version to the stack. <strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see the <em>Security Management System User Guide</em>.</td>
</tr>
<tr>
<td>Stack information</td>
<td>Information</td>
<td>Suggested Action</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
<td>-----------------</td>
</tr>
<tr>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by TOS Versions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Digital Vaccine</strong></td>
<td>Indicates the Digital Vaccine (DV) version for each of the devices. Major indicator 🟢: Mismatch in versions or distribution. <strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by Digital Vaccines.</td>
<td>Distribute the DV package to the stack. <strong>Note:</strong> 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.</td>
</tr>
<tr>
<td><strong>{aux-dv-sub type-name} ThreatDV Versions</strong></td>
<td>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 &lt;None&gt;. Major indicator 🟢: Mismatch in versions or distribution. If a ThreatDV subtype is not distributed to any devices, it is not displayed. <strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by ThreatDV Versions.</td>
<td>Distribute the ThreatDV package to the stack. <strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>Stack information</td>
<td>Information</td>
<td>Suggested Action</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| ![Digital Vaccine Toolkit](image) `{dvt-name}` | 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>`.

Major indicator: Mismatch in distributions (not versions).

If a DVT is not distributed to any devices, it is not displayed.

**Tip:** To filter synchronization information by this type of issue, use the Type column to filter by DVToolkit Versions. | Distribute the DVToolkit package to the stack.

**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*. |

| ![Physical Segment](image) `{physical-segment-name-and-direction}` | Indicates the `{profile name} `{profile-version}` was distributed to a physical segment on each of the devices.

Major indicator: Mismatch between profile name, profile version, or distribution.

Major indicator: `<Unknown>` A profile has not been distributed to a segment on one of the devices.

**Tip:** To filter synchronization information by this type of issue, use | Distribute the profile to the physical segment.

**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*. |
<table>
<thead>
<tr>
<th>Stack information</th>
<th>Information</th>
<th>Suggested Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>the Type column to filter by Physical Segment's Profiles.</td>
<td></td>
</tr>
<tr>
<td>Red {virtual-segment-name}</td>
<td>Indicates the {profile-name} {profile-version} was distributed to a virtual segment on each of the devices. Major indicator ☐: &lt;Unknown&gt; 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. Major indicator ☐: Mismatch between profile name, profile version, or distribution is displayed. There is one row for each virtual segment. Tip: To filter synchronization information by this type of issue, use the Type column to filter by Virtual Segment's Profiles.</td>
<td>Distribute the profile to the virtual segment. 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.</td>
</tr>
<tr>
<td>Yellow Missing {virtual-segment-name}</td>
<td>Indicates a virtual segment exists on the SRD but is missing from all the other stack members. Critical indicator ☑: There is one missing virtual segment row for each virtual segment</td>
<td>Edit and save the virtual segment to update the stack. 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.</td>
</tr>
<tr>
<td>Stack Information</td>
<td>Information</td>
<td>Suggested Action</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>on the SRD that is not on any of the other member devices.</td>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by <strong>Missing Virtual Segment.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Extra <code>{virtual-segment-name}</code></strong></td>
<td>Indicates an extra virtual segment exists on one of the stack members but is missing from the SRD.</td>
<td>Delete the extra virtual segment if it is not applicable. Or, edit and save the virtual segment to update the stack.</td>
</tr>
<tr>
<td><strong>Mismatched group for <code>{virtual-segment-name}</code></strong></td>
<td>Indicates the <code>{segment-group-name}</code> to which a virtual segment belongs for each of the devices.</td>
<td>Edit and save the segment group (without making any changes) to update the segment group with all of its segments.</td>
</tr>
<tr>
<td><strong>Warning:</strong> <strong>Mismatched group displayed.</strong></td>
<td>Mismatch displayed.</td>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>Stack information</td>
<td>Information</td>
<td>Suggested Action</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
<td>-----------------</td>
</tr>
<tr>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by Virtual Segment's Group.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mismatched group for <code>{physical-segment-name}</code></strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicates the <code>{segment-group-name}</code> to which a physical segment belongs for each of the devices.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Critical indicator ✖ Mismatch displayed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is one row for each physical segment that has a mismatch in segment groups.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by Physical Segment's Group.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Edit and save the segment group (without making any changes) to update the segment group with all of its segments.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see the <em>Security Management System User Guide</em>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Extra rule <code>{inspection-bypass-rule-name}</code></strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indicates that there is an inspection bypass rule on a stacking device that is not on the SRD.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Critical indicator ✖ Mismatch displayed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>There is one row for each inspection bypass rule.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by Extra Rule.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Edit and save the inspection bypass rule (without making any changes) to update the stack.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see the <em>Security Management System User Guide</em>.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Stack information

<table>
<thead>
<tr>
<th>Missing {inspection-bypass-rule-name}</th>
<th>Indicates that there is an inspection bypass rule on the SRD that is missing from a device in the stack.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Critical indicator ⚠️ Mismatch displayed.</td>
</tr>
<tr>
<td></td>
<td>There is one row for each inspection bypass rule.</td>
</tr>
<tr>
<td><strong>Tip:</strong></td>
<td>To filter synchronization information by this type of issue, use the Type column to filter by Missing Rule.</td>
</tr>
<tr>
<td></td>
<td>Edit and save the inspection bypass rule (without making any changes) to update the stack.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For information about where the options are different for managing a stack of devices instead of a single device, see the <em>Security Management System User Guide</em>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stack Resilience {stack-resilience-value}</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Critical indicator ⚠️ Mismatch displayed.</td>
</tr>
<tr>
<td><strong>Tip:</strong></td>
<td>To filter synchronization information by this type of issue, use the Type column to filter by Device Resilience Mismatch.</td>
</tr>
<tr>
<td></td>
<td>Edit and save the stack configuration (without making any changes) to update all of the stacking devices.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SSL Enabled</th>
<th>Indicates that SSL inspection is enabled on some of the devices in the stack but not all of them.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Edit the device configuration on each stacking device to verify that SSL inspection is enabled (<em>Devices &gt; All Devices &gt; device-name &gt; Device Configuration</em>). For more information, see the <em>Security Management System User Guide</em>.</td>
</tr>
<tr>
<td>Stack information</td>
<td>Information</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>SSL Licensed</td>
<td>Indicates that some of your devices have a license that allows SSL inspection and others that do not allow SSL inspection.</td>
</tr>
<tr>
<td>License Throughput</td>
<td>Indicates that some of your devices have a license for a different inspection throughput rate than the other devices.</td>
</tr>
<tr>
<td>Extra VLAN</td>
<td>Indicates that there is a VLAN translation rule on a stacking device that is not on the SRD. There is one row for each VLAN translation rule. <strong>Tip:</strong> To filter synchronization information by this type of issue, use the Type column to filter by Extra VLAN.</td>
</tr>
<tr>
<td>Missing VLAN</td>
<td>Indicates that there is a VLAN translation on the SRD that is missing from a device in the stack.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Ready for stacking]</td>
<td>Indicates that there is no issue with adding the device to the stack.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>![This device's TOS version doesn't match the TOS version for the selected devices.]</td>
<td>Indicates that there is a TOS version mismatch.</td>
<td>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.</td>
</tr>
<tr>
<td>![This device does not support stack sizes of more than ## devices.]</td>
<td>Indicates a device is valid for stacking, but that the maximum number of devices in the stack has been reached.</td>
<td>Remove a device from the stack so that you can add the device. See Remove a device from the stack on page 14.</td>
</tr>
</tbody>
</table>
### Status

<table>
<thead>
<tr>
<th>Status</th>
<th>Information</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Device is not communicating" /></td>
<td>Indicates that the device is not communicating with the SMS.</td>
<td>Verify network connectivity between the SMS and the device. Also, verify the required ports are not being blocked. For more information, see the Security Management System User Guide.</td>
</tr>
<tr>
<td><img src="image" alt="Device is unmanaged" /></td>
<td>Indicates that the device is no longer managed by the SMS.</td>
<td>In the SMS, manage the device:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. In SMS tools, click <strong>Devices</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Right-click the unmanaged device and click <strong>Edit &gt; Manage Device</strong>.</td>
</tr>
</tbody>
</table>

## 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 SP ports.

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

<table>
<thead>
<tr>
<th>Inspection Tier</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stack : Segment Ports</td>
<td>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. When stacking is enabled, the following information is displayed:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Segment Rx Mbps</strong> displays the aggregate received traffic from all network segments on this device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Segment Tx Mbps</strong> displays the aggregate traffic transmitted from all network segments on this device.</td>
</tr>
</tbody>
</table>
### Inspection Tier

<table>
<thead>
<tr>
<th>Information</th>
</tr>
</thead>
</table>
| **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.  
  
  ° **<host n> Rx Mbps** displays the traffic balanced from this device's network segments to the other devices in the stack.  
  
  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.  
  
  ° **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

This inspection tier presents SP port throughput, including through traffic and return traffic rates.

When stacking is enabled, the following information is displayed:

<table>
<thead>
<tr>
<th>Information</th>
</tr>
</thead>
</table>
| **Stack Rx Mbps** displays the aggregate received traffic from both SP ports.  
  
  **Stack Tx Mbps** displays the aggregate traffic that is transmitted from both SP ports.  
  
  **Stack Rx > Stack Tx** displays the total amount of transit or through traffic on the SP ports; for example, traffic received on SP 1, which is forwarded by the switch to SP 2.  
  
  **Stack Rx > Seg Tx** displays the amount of return traffic coming in on a SP 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 29.

**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 23.

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 23.

- 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 32.

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.
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

In the SMS, you can collect diagnostic information from an IPS or TPS device by exporting a Tech Support Report (TSR). The TSR collects information from diagnostic commands and log files into a report that TippingPoint product support can use to diagnose issues with the device.

Unlike a TSR created on the device by using the 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 Local Security Manager, see the *Local Security Manager User Guide*. 
**Important:** The SMS exports a TSR from TippingPoint IPS and TPS 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 device 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 product support for assistance. For contact information, go to [https://tmc.tippingpoint.com](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 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**

Use the Command Line Interface (CLI) to display stacking status information on the device. For more information about stacking-related commands, see the *TPS 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) v5.0.0 (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.

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stacking enabled</td>
<td>Indicates whether stacking is enabled on the device.</td>
</tr>
<tr>
<td>Stacking active</td>
<td>Indicates whether stacking is currently functioning.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Information</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Stack member state</td>
<td>Indicates the current working state of this device on the stack.</td>
</tr>
<tr>
<td>Stack master</td>
<td>Indicates whether this device manages the state of the stack.</td>
</tr>
<tr>
<td>Number of devices configured in stack</td>
<td>Indicates the number of TippingPoint TPS security devices that are connected together through the stacking bus.</td>
</tr>
<tr>
<td>Number of devices required in stack</td>
<td>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.</td>
</tr>
<tr>
<td>Advertised state</td>
<td>Indicates the state that the device advertises to the stack master.</td>
</tr>
</tbody>
</table>
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.

- 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 8200TX or 8400TX 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, v5.0.0 or later, must be installed on each TX Series device in the stack.

• The same slot on each device must be configured with either the same network I/O module or no network I/O module as compared to the network segment device. For more information, see Multiple network segment device configuration on page 9.
Stacking terminology

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

**SP port**
An *special purpose (SP) port* is a 40 GbE QSFP+ port that connects each stack member to its peer in a stacking bus. The SP ports directly connect to each device by using an Active Optical Cable (AOC). Do not connect the SP ports through a switch.

**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. You can configure a stack with up to five TippingPoint security devices. In-line inspection capacity increases with each device that you add to the stack.

**stacking bus**
The *stacking bus* consists of two SP ports on each stacking device that connect the stack in a ring topology.