Threat Protection System Release Notes

Version 5.2.0

To ensure that you have the latest versions of product documentation, visit the Online Help Center.

Important notes

This release is supported on vTPS, 440T, 2200T, 1100TX, 5500TX, 8200TX, and 8400TX devices.

- The Release Contents of this document describe features or resolved issues specific to TOS v5.2.0. If you are upgrading from an earlier, nonsequential TOS, refer to the release notes of any interim releases for additional enhancements.
- All TPS devices must be running a minimum of v5.0.1 before installing this version.
- Use SMS v5.2.0 and later to manage a TPS device with this release.

Release Contents

Description	Reference
This release expands the TPS TX Series to include the 1100TX and 5500TX models.	New
This release introduces the 40 GbE Fiber (LR4/SR4) Bypass I/O module (BIOM). Using this bypass I/O module, users can deploy TX devices on a 40 GbE network without any concerns of breaking the network in the event of a device outage. Make sure that you upgrade to TOS v5.2.0 before inserting the 40 GbE bypass module.	New
You can stack nonadjacent TPS 8200TX or 8400TX devices at greater distances using any MSA-Compliant 40 GbE active optical cable (AOC) or QSFP+ transceiver and cable combination.	TIP-29073
TOS v5.2.0 provides support for fixed ethtype inspection bypass that addresses Link Aggregation Control Protocol (LACP) issues.	TIP-26834
For 8200TX and 8400TX devices, VXLAN inspection is supported for UDP ports 4789, 8472, and 48879. This capability is enabled automatically.	TIP-20626
TPS administrators can use the SMS as a remote authentication server.	TIP-29016
vTPS devices support an inspection capacity of 2 Gbps (license required) for both Normal Mode and Performance Mode.	TIP-38132
The TPS warns users when their CLI session has been idle too long and that they will be disconnected.	125351
When the state of a stacking port changes—inserted or removed—an entry is recorded in the system log.	124877
The device no longer generates an `Unexpected unchunking sequence derived` message.	125742
A condition that caused segment ports to disappear after an attempt to install a KVM-deployed vTPS without the correct number of data ports has been repaired.	118728
Issues that caused filters to trigger on inapplicable traffic have been resolved.	124716
In certain scenarios, you no longer have to manually restart inspection ports configured for Link Down Sync (LDS) Wire mode when they become disabled after an LDS event.	TIP-30218
A best effort mode issue that could result in increased latency and reduced throughput without packet loss no longer occurs.	116539
The yellow stacking LED works correctly on 8200TX and 8400TX devices.	TIP-23017

A condition that caused the Module Health LED to turn green prematurely has been addressed.	TIP-26594
This release addresses an issue where the device would erroneously enter Layer-2 Fallback when booting.	TIP-29530
This release prevents an invalid process control block pointer from occurring, which caused TX devices to fail.	TIP-32909
New inner tunnel limits prevent a cross-packet inspection issue.	126189
Use the `show ntp` command to verify that the device and NTP server times are synced.	123466
Hovering the mouse over a filter name in Block/Alert logs no longer displays a 501 filter loading error.	123291

Known issues

Description	Reference
When you insert a 40 Gbps bypass module (BIOM) into a TX-Series TPS device that has not been upgraded to TOS v5.2.0, the module health status LED indicates that the module has experienced a fault (solid amber). To recover from this state: 1. Upgrade the device to TOS v5.2.0. 2. After the upgrade, perform a full reboot of the device. 3. Disable bypass on all BIOMs by selecting the normal option: • SMS: From the Device menu, click the device and select **Device Configuration -> HA (High Availability) -> Zero Power HA**. • LSM: Select **System -> High Availability -> Zero-Power HA**. • CLI: `high-availability zero-power (bypass|normal) (slot|all)`	TIP-33655
For optimal performance of URL filtering and other memory intensive features running on a vTPS in Normal mode, configure 16 GB of RAM.	TIP-33876
Data might stall on long-lasting persistent connections with infrequent traffic that go through SSL inspection.	TIP-34514
System logs do not indicate when a device is forced into a cold reboot.	TIP-31776
eVR scans do not support non-ASCII characters in filenames.	TIP-35729
If a TPS device ever experiences a core dump, every subsequent technical support report (TSR) includes a core dump file.	TIP-31585

Adding or deleting inspection bypass rules can cause the remaining rules to be reordered differently than the way they were listed in the original configuration. Reboot the device to restore the originally configured order.	TIP-30537
When you create a snapshot using the LSM, the browser sometimes times out even though the snapshot creation eventually succeeds.	TIP-37112
Placing an inspection bypass rule with an ingress-mirror action first in the rule order can change the behavior of subsequent rules.	TIP-36974
System logs do not indicate when the state of a transceiver changes.	TIP-39167

Product support

For assistance, contact the *Technical Assistance Center (TAC)*.