Threat Protection System Release Notes

Version 5.5.2

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.

- 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 v5.4.0 before installing this version. Learn more.
- Use SMS v5.5.2 and later to manage a TPS device with this release. SMS v5.5.2 upgrades are only supported from an SMS installed with SMS v5.3.0 or later. Attempts to upgrade from an older release will return an error. If the error message is blank, check the SMS system log for the complete message.

Release Contents

Description	Reference
This release fixes an issue that caused an `Unable to fetch ips-profile list to validate configuration` system log message.	TIP-67191 SEG-111905
After upgrading to v5.5.0, some customers experienced unexpected packet blocks for filter 7704, which triggered further transmissions. This issue is fixed in this release.	TIP-70597 SEG-119519
This release fixes a rare task crash that some devices experienced during high traffic load while processing a TLS handshake.	TIP-69516 SEG-116764
Some devices failed to provide any SNMP interface statistics, and SNMP statistics for 40 GB IOMs were not handling unpopulated interfaces in an IOM slot correctly. This issue is fixed in this release.	TIP-65670 SEG-95791
This release fixes an issue that caused some customers to report unexplainable license utilization statistics.	TIP-70454
The maximum transmission unit (MTU) increased from 9050 to 9234 bytes on the 1100TX, 5500TX, 8200TX, and 8400TX models.	TIP-70557

Known issues

Description	Reference
Performing a system shutdown on a 2200T device using the SMS or the CLI causes the system to reboot instead of keeping the system powered down.	SEG-115592
When you insert a 40 Gbps bypass module (BIOM) into a TX-Series TPS device that has not been upgraded to at least 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 or later. 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

SSL inspection cannot occur when web mode is enabled. By default, web mode is disabled.	TIP-64243
1G fiber module does not support auto-negotiation. SMS will currently report auto-negotiation as enabled; however, any changes from SMS, LSM, or CLI will not take effect.	TIP-66924
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
In rare occurrences, the TPS does not decrypt sites and the connection will be blocked. If this occurs for sites that must be accessed, navigate to **Profiles > Shared Settings > SSL > Client > Decryption Policies > Domains** on your SMS and specify those sites in the do-not-decrypt list.	TIP-45656 TIP-49103
Deploying a vTPS in Performance mode fails when using version 6.7 of the ESXi Hypervisor. **Workaround:** To successfully complete a deployment in Performance mode using ESXi 6.7, follow these steps: 1. Deploy the vTPS in Normal mode. 2. Shut down the vTPS virtual appliance. If the appliance is managed, you can also shut it down from the SMS client by right-clicking the device on the Devices page and selecting **Edit > Device Configuration**. 3. Configure the vTPS parameters to 6 vCPUs and 16 GB memory. 4. Reboot the vTPS virtual appliance. The SMS automatically recognizes the resource allocation and changes to Performance mode. 5. Examine the output of the `show version` command to confirm that the device is now running in Performance mode.	SEG-76770
System logs do not indicate when the state of a transceiver changes.	TIP-39167
The TPS presents an untrusted certificate warning for some websites because it cannot verify the certificate chain. Administrators of these websites might not be aware that their sites are not configured with a proper certificate chain, since most browsers have developed ways to automatically work around this issue. Consider the following options for accessing such a website: • Use mechanisms specific to your browser to bypass the `Untrusted certificate` warning (for example, add an exception or proceed to the site anyway) • Have your administrator manually download an intermediate certificate, upload it to your device, and add it the Trust Store on your SMS. • Consider providing feedback to the website to inform its administrators that their site employs a misconfigured certificate chain.	TIP-37062

Product support

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