Threat Protection System Release Notes

Version 5.5.3

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 v5.5.3 and later to manage a TPS device with this release. SMS v5.5.3 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
TSRs now include relevant directory information for any partition that is at a critical threshold. The `partition_full.txt` in the TSR contains this information.	TIP-74114 SEG-116874
You can now select whether all crash reports or just the most recent crash reports since the last one are included in TSRs.	TIP-75867
Logs now indicate whenever a transceiver is inserted or removed from a device.	TIP-39167 SEG-49377
You can avoid parsing errors in the remote syslog server by removing excess spaces from the message field of the device's audit and system logs.	TIP-73837 SEG-126268
An issue that prevented auto-negotiation from working for optical SFPs inserted in the 6-segment 1G I/O module on 1100TX and 5500TX TPS platforms has been resolved.	TIP-73790 SEG-117515
This release improves the performance of the scan/sweep feature, including its interoperability with the TLS Inspection feature.	TIP-74665 TIP-74666 TIP-74667 TIP-74668
SCTP traffic processing by the device no longer impacts IPS performance.	TIP-66982
After a reboot, reputation profiles that were set to pending block behavior would change to pending allowed behavior until the SMS preformed a profile distribution. This could result in intermittent reputation leaks.	TIP-73838 SEG-119439
Some users noticed constant alerts generating from the "7703: SMB excessive header padding" filter after an upgrade.	TIP-77795 SEG-135571

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
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

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
For 8200TX and 8400TX TPS models that use the 6-segment 1G I/O module, auto-negotiation is only supported if the SFP type is 1000-BaseT copper. Optical SFPs do not support auto-negotiation under these circumstances.	SEG-145222

Product support

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