Intrusion Prevention System
Release Notes

Version 3.9.3

To ensure that you have the latest versions of product documentation, download the documents from the *Threat Management Center*.

Important notes for IPS

- After installing this release, update the DV package to the latest version.

- Use SMS v4.5.0 and later to manage a device with this release.

- Before you upgrade your device to the latest TOS, maximize the space on your device by removing outdated TOS versions and packet traces that are no longer required. This ensures a successful upgrade and allows for a TOS rollback, if necessary. You can remove previous TOS versions using the SMS, the LSM, or the CLI.

Release Contents

Description	Reference
Improvements to profile distribution times are included in this release.	122838 119064
This release corrects an issue in which the device unexpectedly entered Layer-2 Fallback mode while inspecting particular RFC822 traffic, and created DP Watchdog errors in the system log. The device now inspects RFC822 traffic without issues.	121656
An issue that triggered false positives on filters 11403 and 7704 has been resolved.	119451
Polling of TPS OIDs no longer results in SNMP failures on N-series IPS devices.	121070
SMS virtual segment definitions now persist during routine SMS usage and after restarts. Previously, the system would timeout when configuring or modifying virtual segment precedence in deployments with large numbers of virtual segments.	120870
An issue that could cause inconsistent DNS reputation blocking on NX devices has been addressed in this release.	121860
An SNMP discovery failure no longer occurs after 49 days when a device is configured for SNMP v3 only.	117453
The message *Error reading stream header information* is now a warning level message that has been more accurately worded. Previously, this error level message read *Error reading stream magic*.	121368
Irregular character strings no longer appear in the audit log.	121678
A refresh of adaptive filters from the Member Summary tab no longer clears the list of filters and devices.	117413
System log now limits NTP frequency errors to once every 15 minutes.	118876
Device management no longer reports "Socket Closed" after a TOS upgrade. Customers running TOS versions earlier than 3.8.4 can now directly upgrade to this release.	117565
An issue in which the NXDOMAIN response was not always issued when a packet was dropped due to DNS Reputation has been addressed in this release.	118722
From SMS, you can now clear the red syslog LED on the front panel of an NX device.	119889

Known issues

Description	Reference
When your device is configured to connect to an NTP server using the server hostname, when you reboot the device, the device no longer connects to the NTP server. To avoid this issue, always establish an NTP server connection using the IPv4/ IPv6 address of the NTP server.	118020
Microsoft Edge or Microsoft Internet Explorer might not connect to the LSM. To resolve this issue, use the `conf t server` TLS command to enable TLS v1.0 on the IPS security device or use the Mozilla Firefox browser. For more information about using this command, refer to the *IPS Command Line Interface Reference*.	117878
In certain cases, SMS may reorder virtual segments incorrectly. This only occurs when SMS manages a device and a new ANY-ANY segment is created. This causes a conflict with special reserved security zone pair IDs. To clear the condition, reset the IPS filter settings.	116675
Modifying a profile or changing which profile is applied to the ANY-ANY virtual segment of a device, *while that device is unmanaged from SMS*, can cause an out-of-sync condition when the device is re-managed to the SMS. The recovery for the out-of-sync condition is to reboot the device. To avoid this condition, make changes to the ANY-ANY virtual segment only through the SMS.	124603

Product support

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