ExtremeCloud OS ONE SD-WAN v30.26.2.0 Release Notes

New Features, Improvements, and Known Issues

9041214-00 Rev. AB

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

Abstract

This release notes document for ExtremeCloud OS ONE SD-WAN version 30.26.2.0 provides technical information for network administrators, engineers, and advanced operators on new capabilities, addressed defects, known issues, operational limitations, and upgrade considerations in Fabric-only deployments. It introduces firmware image verification using digital certificates to validate software integrity, USB 5G/LTE modem support for WAN connectivity and failover, Adaptive QoS shaping based on uplink and remote-site bandwidth awareness, XSE-600 platform support with configurable port mapping, per-interface BFD timer profiles, granular LLDP controls, enhanced 5-minute monitoring timelines with real-time troubleshooting, and redesigned tunnel visibility tools for overlay diagnostics. The release also adds downgrade restrictions to ensure configuration consistency. The document details numerous resolved issues involving VPP services, IPsec tunnels, BGP and IS-IS adjacencies, LLDP processing, application visibility, throughput reporting, VLAN interfaces, and appliance stability across supported platforms. Known issues include route withdrawal failures, IS-IS instability under extreme UDP loads, rollback-related configuration loss, temporary deployment status inconsistencies, application flow display limitations, and troubleshooting data refresh requirements. Security considerations include certificate-based firmware validation, while operational guidance covers WAN optimization, LTE deployment scenarios, configuration recovery procedures, upgrade workarounds, and platform-specific limitations such as Adaptive QoS support exclusions. The release notes provide concise diagnostic, recovery, and workaround instructions to support deployment, maintenance, and troubleshooting activities.

General Release Information

Version 30.26.2.0 supports Fabric mode only. Non-Fabric features and configurations are not supported in this release.

New Features in ExtremeCloud OS ONE SD-WAN 30.26.2.0

New features in release 30.26.2.0

Feature ID	Feature	Description	Supported Platforms
SWAN-233	Firmware Image Verification	Firmware images are now verified using digital certificates to ensure that they are from a trusted source and have not been tampered with. The verification occurs automatically during firmware upgrades and requires no configuration. If firmware verification fails, the firmware upgrade workflow displays a **Verification Failed** status, indicating that the firmware image did not pass certificate validation. Firmware Image Verification applies only to firmware versions 30.26.2 and later. Firmware versions earlier than 30.26.2 cannot be verified using this mechanism.	Ipe 40ax V2 Ipe 420ax Ipe-2200ax-F Ipe-2200ax-T XSE-600
SWAN-92	USB/LTE Modem Support	Support for USB 5G/LTE modems (Fujisoft FS040U) on IP40axV2 and IP420ax devices, enabling flexible WAN connectivity for branch deployments. The modem can be configured as a primary WAN connection or as an automatic backup when primary links fail. The modem integrates with all existing SDWAN management and monitoring capabilities, including policy routing, SLA monitoring, and tunnel management. IPv6 is supported with automatic public IP address assignment from the carrier. The system automatically re-establishes	Ipe 40ax V2 Ipe 420ax

Feature ID	Feature	Description	Supported Platforms
		tunnels when carrier-initiated disconnects occur and includes scheduled reconnection to reset carrier lease timers.	
SWAN-162	Adaptive QoS Shaping	Adaptive QoS considers both your local uplink capacity and remote site downlink availability when making traffic-shaping decisions. This prevents congestion at remote sites when their wide area network (WAN) links become saturated and improves application performance across your network. Adaptive QoS dynamically adjusts traffic shaping based on link utilization information exchanged between appliances. By default, Adaptive QoS is disabled. You can enable it through templates or configure it directly on each appliance in General Settings.	Ipe 40ax V2 Ipe 420ax Ipe-2200ax-F Ipe-2200ax-T XSE-600
SWAN-237	XSE-600 Support	XSE-600 appliances type supports configurable port mapping, allowing you to assign fiber (1/10G SFP+) or copper (1/2.5G) ports to interface roles based on site cabling requirements. Each port group includes one fiber port and one copper port, and only one port in each group can be active at a time. ExtremeCloud SD-WAN OS ONE enforces port-mapping constraints to maintain connectivity, including keeping at least one WAN port active and requiring Port 2 or Port 7 in the WAN mapping. Templates now require an explicit platform type selection (XSE-600 or IPE). When replacing an appliance with an XSE-600, select a template that is compatible with the XSE-600 platform.	XSE-600

Feature ID	Feature	Description	Supported Platforms
SWAN-52	BFD Configurable Timers and Per-Interface Profiles	BFD transmit interval and multiplier values are configured per WAN interface, allowing you to optimize failure detection for different link types. Appliance-level settings can override template-level BFD settings. BFD session status and timer values are available in the **BFD Peer Table**. Alerts are generated when BFD adjacency status changes and are automatically cleared when the session recovers.	Ipe 40ax V2 Ipe 420ax Ipe-2200ax-F Ipe-2200ax-T XSE-600
SWAN-235	Granular LLDP Control	Link Layer Discovery Protocol (LLDP) can now be enabled or disabled on individual WAN interfaces directly from the template and appliance configuration. LLDP is enabled by default on all WAN interfaces to support neighbor discovery. A new LLDP toggle is available for each WAN interface. In templates, you can configure it under Additional Settings. At the appliance level, the toggle appears in the Interface section. At the appliance level, you can override template values. This LLDP setting is not applicable to WAN4 (USB/LTE) interfaces.	Ipe 40ax V2 Ipe 420ax Ipe-2200ax-F Ipe-2200ax-T XSE-600
SWAN-238	5-Minute Timeline and Real-Time Troubleshooting	A 5-minute timeline is now available in Flow and Alarm Dashboards, providing a granular view of recent network activity and alarms for faster incident detection. The 5-minute timeline is supported in Site Dashboard, Sites 360, Application 360, and WAN 360. Real-Time Troubleshooting provides a live view of active traffic to help identify and resolve network issues. It is available only when the 5-minute timeline is selected.	Ipe 40ax V2 Ipe 420ax Ipe-2200ax-F Ipe-2200ax-T XSE-600

Feature ID	Feature	Description	Supported Platforms
SWAN-122	Advanced Troubleshooting	The Tunnel Table has been redesigned to provide clearer visibility into SD-WAN overlay connections. The updated view now clearly identifies tunnel initiators, responders, and overlay network membership, making it easier to trace connectivity paths and troubleshoot tunnel establishment issues.	Ipe 40ax V2 Ipe 420ax Ipe-2200ax-F Ipe-2200ax-T XSE-600
XCW-9704	Restrict Firmware Downgrade	To maintain system stability and prevent compatibility issues, firmware downgrades from 30.26.2.0 must follow a mandatory intermediate step. If you need to downgrade to a version earlier than 30.26.1.0, you must first downgrade to 30.26.1.0, then downgrade again to your target version. This two-step process ensures that all configuration and state data are properly handled during the transition.	Ipe 40ax V2 Ipe 420ax Ipe-2200ax-F Ipe-2200ax-T

Addressed Issues in ExtremeCloud OS ONE SD-WAN 30.26.2.0

Addressed issues in release 30.26.2.0

Issue ID	Description
CFD-18015	The **vpp-sdwan** service crashed due to a VPP API error and caused an unexpected reboot on Ipe 40ax V2 appliances.
CFD-18009	The k3s runtime failed to destroy the network sandbox on Ipe 40ax V2 appliances, causing loss of management connectivity and an unresponsive CLI.
CFD-17968	The **vpp-sdwan** service became unhealthy on Ipe 40ax V2 appliances and triggered unexpected reboots.

Issue ID	Description
CFD-17934	An Ipe 40ax V2 appliance remained disconnected from ExtremeCloud OS ONE SD-WAN after an upgrade to version 30.26.1.0, even though IPsec tunnels and user traffic remained operational.
CFD-17894	An LLDP processing error caused an Ipe 420ax appliance to reboot unexpectedly.
CFD-17857	VPP API errors disrupted IS-IS and BGP adjacencies on Ipe 40ax V2 appliances and triggered corresponding alarms.
CFD-17830	Configuring a VLAN ID on WAN1 of an Ipe 420ax appliance caused ExtremeCloud SD-WAN to display the connection status as **Unknown**, even though IPsec tunnels and traffic remained operational.
CFD-17741	An Ipe 40ax V2 appliance rebooted unexpectedly without an identifiable cause.
CFD-17739	High CPU and memory utilization caused an Ipe 40ax V2 appliance to reboot unexpectedly.
CFD-17727	SD-WAN alarm notification emails displayed the **Last seen** value as a UNIX timestamp instead of a readable date and time.
CFD-17666	Ipe 40ax V2 appliances experienced high memory and CPU utilization along with WAN link failures.
CFD-17565	ExtremeCloud SD-WAN OS ONE could incorrectly display an appliance as **Disconnected** even though the appliance was connected and communicating with the service.
CFD-17383	The **vpp-sdwan** service terminated and caused an IPE 420AX appliance to reboot unexpectedly.

Issue ID	Description
CFD-17201	ExtremeCloud OS ONE SD-WAN displayed an appliance as **Connected**, while ExtremeCloud IQ did not display the appliance in Inventory.
CFD-17135	The **vpp-sdwan** service became unhealthy and caused an Ipe 2200ax-F appliance to reboot unexpectedly.
CFD-17113	The appliance generated false LLDP neighbor alerts after a software upgrade even though the neighbors remained connected.
CFD-17099	ExtremeCloud OS ONE SD-WAN generated a **No Default Gateway** alarm across multiple sites without an underlying gateway failure.
CFD-16897	IPsec tunnels went down when the IPv6 prefix on a WAN interface changed through IPoE (RA), because the appliance continued using the old IPv6 address as the tunnel source.
CFD-16857	The Cleared Alarms view took approximately 30 seconds to load the **Filters** tab and displayed errors while loading the filter options.
CFD-16751	The appliance reported an incorrect reboot reason and inconsistent reboot information after an upgrade.
CFD-16685	Ipe 40ax V2 and Ipe 420ax appliances experienced unexpected reboots after an upgrade to version 30.25.5.0.
CFD-16637	ExtremeCloud OS ONE SD-WAN stopped displaying applications and application flows after an appliance upgrade.
CFD-16575	An appliance lost IS-IS adjacency after an upgrade and required a reboot to restore the adjacency.

Issue ID	Description
CFD-16567	The ExtremeCloud OS ONE SD-WAN web interface could not download large automatically generated TechSupport files.
CFD-16446	BFD session instability caused IS-IS adjacency to flap on appliances using Fabric Extend.
CFD-16240	ExtremeCloud OS ONE SD-WAN stopped displaying applications and application flows after an upgrade from version 30.25.4.0 to 30.25.5.0.
CFD-16214	An unexpected appliance reboot left IS-IS adjacency and LLDP interfaces down, causing traffic impact.
CFD-16192	The **vpp-sdwan** service consumed excessive CPU resources and triggered an unexpected reboot on ipe-2200ax-F appliances.
CFD-16030	ExtremeCloud OS ONE SD-WAN did not display site-level throughput even though the appliance forwarded traffic.
CFD-15681	Core switches at the site reported an **SPBM detected adjacency Down** event, causing IS-IS/SPBM adjacency loss between the SD-WAN overlay and Fabric switches. Rebooting the ExtremeCloud OS ONE SD-WAN appliances restored the adjacency.
CFD-15068	After an upgrade to 30.25.4.0, the ExtremeCloud OS ONE SD-WAN appliance displayed incorrect port mappings, including an incorrect physical interface assignment for LAN1 and WAN2.
XCW-9384	The appliance listing page displayed a firmware upgrade status of **Failure** with the reason **Aborted**, even though the appliance successfully upgraded to the requested firmware version.
XCW-9337	The hub appliance continued to report an incorrect tunnel count for WAN connections after the corresponding spoke WAN configuration was removed from the template.

Issue ID	Description
XCW-9332	Configuration deployment failed when the DHCP Lease Time (Option 51) was configured between 31,536,001 and 31,622,400 seconds (more than 365 days and up to 366 days).
SDW-2243	Overlay IP connectivity was lost after route-based tunnel configuration changes. BGP and BFD sessions were not established, and tunnel information was not updated correctly.
SDW-2241	During the initial establishment of certain HTTPS sessions, the DPI engine initially classified traffic with a generic application identifier, such as **google_gen**, before identifying the specific application. When Dynamic WAN Selection (DWS) used session-based path selection, the initial classification determined the WAN path for the duration of the session, even after the DPI engine identified the correct application.
SDW-2163	Link metrics reported 100 percent loss for UDP iPerf traffic even though the traffic was successfully transmitted. This occurred when upstream and downstream ExtremeCloud OS ONE SD-WAN appliances identified the iPerf traffic differently, causing inconsistent application classification and incorrect loss reporting. Link metrics now report UDP iPerf traffic correctly.
SDW-2076	Traffic statistics were not displayed for logical network interfaces (VLAN subinterfaces) when traffic passed through tagged interfaces because the appliance did not collect or export traffic counters for VLAN subinterfaces.
SDW-2095	IP address configuration on tagged or untagged WAN subinterfaces could not be modified when the initial configuration used the CLI and a subsequent configuration change used ExtremeCloud OS ONE SD-WAN. Attempts to change between static IP addressing and DHCP or auto-configuration failed or were not applied as expected.
SDW-1321	DTI reply traffic failed to forward after SD-WAN static routes were advertised to the Fabric Extend network. DTI reply traffic now forwards correctly after advertising ExtremeCloud OS ONE SD-WAN static routes to the Fabric Extend network.

Issue ID	Description
CFD-16870	The ExtremeCloud OS ONE SD-WAN Ipe 40ax and Ipe 420ax appliances intermittently remained unresponsive during the system reload sequence following a software upgrade, requiring a manual power cycle to recover. This occurred because a hardware watchdog issue on these specific models failed to trigger an automatic system reset when the reload stalled.
CFD-18092	The BFD and BGP sessions intermittently dropped or remained down on SD-WAN appliances following an IPsec rekey event due to a Security Association (SA) programming failure. This caused stale SA entries to persist, resulting in loss of overlay reachability. An appliance reboot was required to restore connectivity.
CFD-16899	ExtremeCloud OS ONE SD-WAN Ipe 2200ax appliances intermittently experienced an unexpected system panic reboot due to an internal service health check failure.
CFD-17717	The appliances experienced unexpected IS-IS/SPBM adjacency failures and temporary traffic loss across hub and spoke sites.
CFD-17485	The ExtremeCloud OS ONE SD-WAN Ipe-2200ax-F appliance unexpectedly experienced a system panic reboot with the error `vpp-sdwan service not healthy`.
CFD-16500	ExtremeCloud OS ONE SD-WAN appliances experienced intermittent BFD flaps and IS-IS adjacency failures during IPsec Child SA rekey events.
SDW-1164	Disabling a WAN interface in an Orchestrator template and deploying the updated configuration caused a deployment failure with the error: `Neighbor <IP> is already member of <peer-group> peer group`.

Known Issues in ExtremeCloud OS ONE SD-WAN 30.26.2.0

Known Issues in release 30.26.2.0

Issue ID	Description
SDW-3024	Static-network public routes are not withdrawn when tracker-IP reachability is lost. **Symptom** When the last reachable DTI interface loses reachability, the associated static network

Issue ID	Description
	routes are not withdrawn from the routing table. Stale routes remain installed and continue to be advertised and used for forwarding, resulting in traffic being forwarded to an unreachable next hop. This causes internet traffic loss and connectivity disruption. **Condition** This issue occurs when: • One or more static network routes are configured and associated with DTI reachability. • Multiple DTI interfaces are present, but the last remaining reachable DTI interface transitions to an unreachable state. • After the final DTI interface loses reachability, the system fails to update the route state and does not withdraw the affected static network routes from the routing table. **Workaround** Restore reachability on at least one DTI interface.
SDW-2979	IS-IS adjacency drops under excessive UDP traffic. **Symptom** The IS-IS adjacency goes down when the device experiences a massive overload of UDP traffic. IS-IS adjacencies remain stable when traffic rates stay below the configured max-ingress bandwidth. The system remains stable at two times the configured limit. The IS-IS adjacency drops specifically when UDP traffic reaches or exceeds three times the configured max-ingress limit. **Condition** Incoming UDP traffic rate is sent at three times (or more) the configured max-ingress bandwidth on an LTE WAN interface. **Workaround** Update the max-ingress bandwidth configuration to match the actual incoming traffic rate. **Recovery** Reduce the incoming traffic rate as per the configured max-ingress bandwidth.

Issue ID	Description
SDW-3105	Device disconnects from orchestrator after rolling back from version 30.26.2.0 to 30.25.x. **Symptom** Device disconnects from the orchestrator after rolling back from version 30.26.2 to 30.25.x. Interfaces either display missing Day1 configurations (example: static IP addresses used to connect to orchestrator in 30.26.2) or appear in shutdown state. **Condition** Firmware rollback is performed from 30.26.2 to 30.25.5.1. During rollback, only Day0 configuration is restored. Any Day1 configurations (such as static IP addresses, VLAN settings, DNS servers) made in the previous version are not restored. If Day1 configurations are required for orchestrator connectivity, the device cannot reconnect. Additionally, if Day0 configuration fails to restore during rollback, all interfaces are in shutdown state, and the device has no connectivity. **Workaround** Direct rollback or downgrade from version 30.26.2 to 30.25.x is not supported. If performed, apply one of the following workarounds based on your configuration: • If the device was using Day0 configuration (DHCP) for orchestrator connectivity in the previous version, the rollback should succeed with no further action required. • If Day1 configurations (static IP addresses, VLAN settings, DNS servers, and so on) were in use and are missing after rollback, manually reconfigure these Day1 settings through the CLI to restore orchestrator connectivity. • If all interfaces are in shutdown state after rollback, access the device through the console and run the following command to restore Day0 configuration: copy default configs running-config This is sufficient if no Day1 configurations were in use. If Day1 configurations were in use, reconfigure them through the CLI to restore orchestrator connectivity. **Recovery** To prevent this issue, do not perform direct downgrades or rollbacks from version 30.26.2 to 30.25.x. Before attempting any downgrade or rollback: • Document all Day1 configurations (static IP addresses, VLAN settings, DNS servers, gateway settings, and so on) if they were in use in the previous version. • Maintain a backup of your configuration.

Issue ID	Description
	• Ensure console access to the device is available for recovery purposes. If a downgrade is unavoidable: • Understand that only Day0 configuration is restored after rollback. • If Day1 configurations were in use in the previous version, reconfigure them through the CLI to restore orchestrator connectivity. • If all interfaces are in shutdown state, use console access to run the following command to restore Day0 configuration: copy default configs running-config. • If Day1 configurations were previously in use, reconfigure them to restore orchestrator connectivity.
SDW-3125	High Throughput and Session Count Spike on Spoke after Hub reboot. **Symptom** A Spoke appliance may experience intermittent spikes in throughput and session count immediately after the Hub reboots. Elevated Kafka metrics may occur concurrently with the spikes. **Condition** This issue occurs when the Hub uses WAN4 (LTE) as the active tunnel underlay when it reboots. The issue does not occur when the Hub uses wired WAN interfaces (WAN1–WAN3). **Workaround** If possible, avoid using Hub WAN4 (LTE) as the primary tunnel underlay. Configure a BGP Local Preference of **10** for WAN4 so that the appliance uses it only as an emergency backup when all wired WAN links are unavailable. If you plan to reboot the Hub, schedule the reboot during a low-traffic period to minimize the impact of the temporary spike. **Recovery** Traffic and session count automatically return to normal after the Hub reboot completes. No manual intervention is required.

Issue ID	Description

SDW-3037	IPv6 Neighbor Entry Shows REACHABLE State Instead of PERMANENT After Remote Link Flap
	
	Symptom
	After a remote link flap (shut/no-shut on the connected switch), the IPv6 neighbor (ARP) entry for the default gateway in the kernel shows state **REACHABLE** instead of the expected **PERMANENT** state.
	
	Condition
	This issue occurs on Ipe 420ax appliances with IPv6 autoconfiguration enabled on the WAN interface when:
	• The remote peer (for example, a Fabric switch running as an RA server) performs a link flap (shut/no-shut).
	• There is a large gap between the shut and no-shut. The interface restarts fresh, sends a Router Solicitation (RS), and the RA reply from the peer carries the gateway's MAC. The kernel fills the neighbor entry itself, bypassing ARPND, which results in REACHABLE state.
	• If the gap is small, ongoing traffic triggers a Neighbor Solicitation (NS) from the kernel through the pkt driver and ARPND path, which correctly sets the state to PERMANENT.
	
	Workaround
	Perform a local interface shut/no-shut on the SDWAN appliance:
	
	`ethernet 0/x shutdown`
	`no shutdown`
	
	This triggers the kernel to initiate a Neighbor Solicitation (NS) which follows the ARPND path and restores the entry to PERMANENT state. There is no functional traffic impact while the entry is in REACHABLE state — it is a transient kernel-managed state that may self-correct when the kernel next queries the neighbor.

Issue ID	Description
XCW-9816	Configuration Status temporarily shows Failed after deployment. **Symptom** The Configuration Status on the Appliance List screen temporarily changes to **Failed** after deployment, even though the deployment completes successfully. The status automatically updates to **Updated** after some time. **Condition** This issue occurs occasionally when the configuration deployment takes longer than expected. **Workaround** Redeploy the configuration. A second deployment resolves the issue, and the configuration status updates to **Updated**.
XCW-9813	Application Flows table not visible at 100% browser zoom with specific display settings. **Symptom** The Application Flows table under Applications > Monitoring is not visible when the browser zoom is set to 100%. **Condition** This issue occurs when the display resolution is 1920 x 1080 with the display scale set to 125% and the browser zoom set to 100%. **Workaround** Reduce the display resolution scale, reduce the browser zoom level, or hide the timeline to restore visibility of the Application Flows table.
XCW-9812	Advanced Troubleshooting tables show no data on first load. **Symptom** When opening the Advanced Troubleshooting page for the first time, the tables for Network Interfaces, Tunnels, Routing, and Additional Services do not display any data. **Condition** This issue may occur due to a timing issue in the appliance-orchestrator communication, where the first backend call for stats returns empty data.

Issue ID	Description
	Recovery Select **Refresh** on the **Advanced Troubleshooting** window to reload the data.
SDW-1457	RTG throughput graphs may show fluctuations during congestion when steady traffic is mixed with intermittent flows, including flows not configured from the Orchestrator. Top-priority traffic always receives the required bandwidth (maximum or objective) as long as total demand is within limits. If demand exceeds capacity, bandwidth is reduced proportionally, prioritizing top-priority traffic. When only one traffic type is present, the system allocates maximum bandwidth; with multiple types, it follows maximum or objective bandwidth unless load forces proportional reduction. **Workaround** Ensure continuous traffic across all flows to stabilize RTG throughput graphs. **Recovery** Stop intermittent traffic or maintain continuous traffic across at least two flows.
XCW-9879	False Configuration Failure Alarm After Upgrade to 30.26.2.0. **Symptom** After upgrading the orchestrator from 30.26.1.0 to 30.26.2.0, a false alarm indicating **Configuration Failure** is raised. However, on the Appliance Listing page, the Configuration Status for all appliances is correctly displayed as **Updated**. **Condition** This issue is intermittently observed after an orchestrator upgrade from 30.26.1.0 to 30.26.2.0. **Workaround** Perform one configuration deploy. After the deployment, the false alarms are moved to the cleared section. **Recovery** The false alarm is automatically cleared after the next configuration deployment. No additional intervention is required.

Limitations in ExtremeCloud OS ONE SD-WAN 30.26.2.0

Adaptive QoS

Adaptive QoS is not supported on WAN 4 (LTE).

Upgrade failure after factory reset

After performing a factory reset, upgrading the appliance from release **30.25.4.0** to **30.26.2.0** may fail with the following error message:

```
NOT_FOUND: download failed. error: rpc error: code = Unknown desc =
stat /var/data/cert-mgmt/ca-trust/ca-list.pem: no such file or
directory.
```

Workaround:

Create an empty file on the appliance before initiating the upgrade:

```
touch /var/data/cert-mgmt/ca-trust/ca-list.pem
```

Global Support

By Phone: +1 800-998-2408 (toll-free in U.S. and Canada)

For the toll-free support number in your country:
https://extremeportal.force.com/

By Email: support@extremenetworks.com

By Web: https://extremeportal.force.com/

For information regarding the latest software release, recent release note revisions and documentation, or if you require additional assistance, please visit the Extreme Networks Support website.