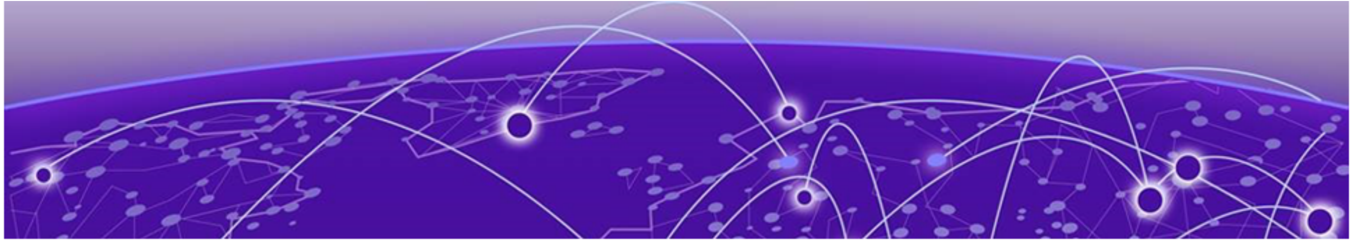
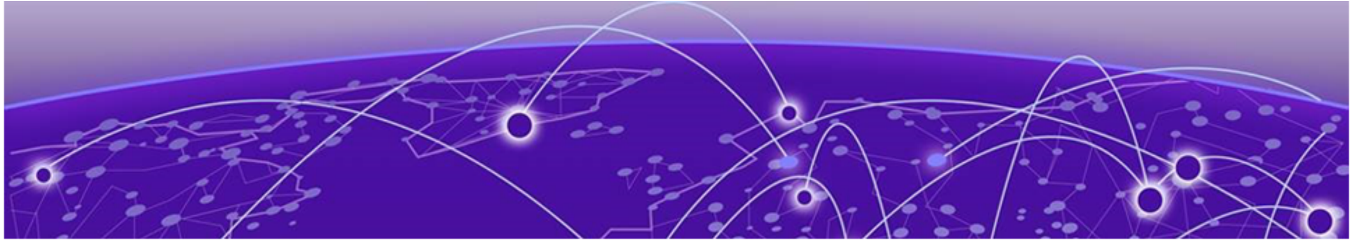
# Extreme ONE OS Switching v22.2.0.0 Release Notes

## New Features, Bug Fixes, and Known Limitations

9039339-00 Rev AA
July 2025



# Table of Contents



# Legal Notices

## 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

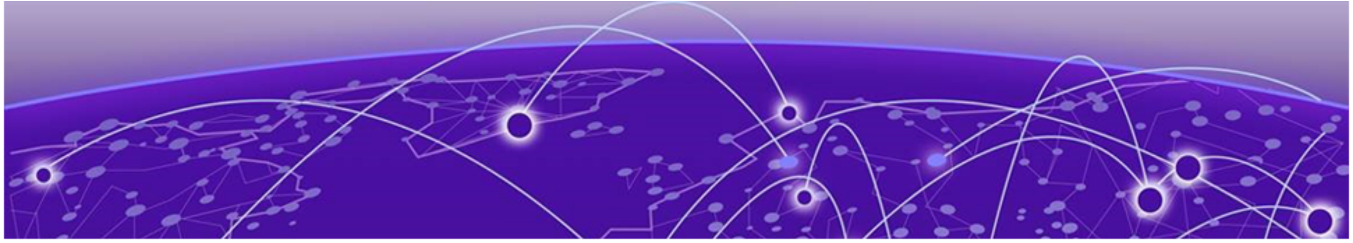
Extreme Networksand the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

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

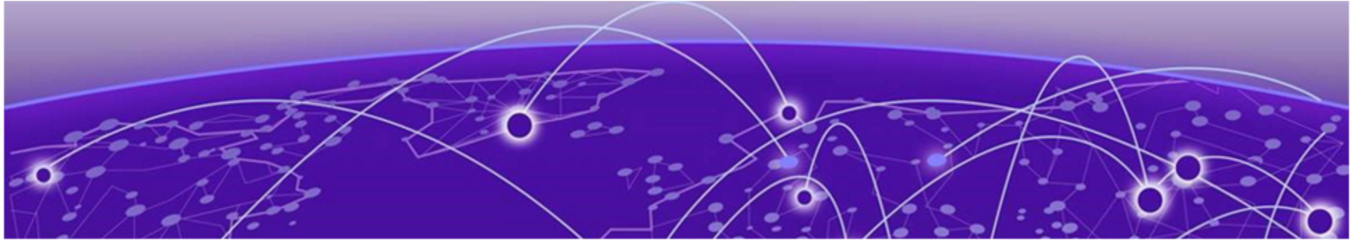
## Open Source Declarations

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

The Extreme ONE OS v22.2.0.0 Release Notes provides a comprehensive overview of new features, bug fixes, and known limitations for the latest version of the operating system designed for IP fabrics and data centers. Key technical features include support for various transceivers, hardware components, dual management interfaces, and key system health indicators. Detailed capabilities of the Baseboard Management Controller (BMC), image management, logging infrastructure, user management, and network protocols such as SNMP, NTP, TACACS+, LDAP, SSH, Telnet, and RADIUS are provided. Advanced functionalities like certificate management, token management, Python script execution, and mutual TLS for secure connections are also covered. Supported features for link layer discovery, static routing, quality of service, access control lists, and BGP routing policies are highlighted. Known limitations include restrictions on SNMP set support, static routing features, and certain BGP underlay functionalities. Open defects are listed, and guidance on obtaining technical support from Extreme Networks is provided.



# Release Notes

## Introduction to Extreme ONE OS

Extreme ONE OS is a cloud-native network operating system (NOS) based on a micro-services architecture. Key characteristics include:

- Modular and composable design for a simple software life-cycle management.
- API-first approach for management programmability.
- Data plane abstraction, supporting integration with multiple ASIC vendors and accelerating the introduction of new hardware platforms.
- Security-first principles that enhance responsiveness to vulnerabilities and minimize the attack surface.

Extreme ONE OS is a high-performance network operating system designed for data centers, service provider, and enterprise networking environments. Extreme ONE OS powers Extreme 8000 series switches and routers.

## Supported Features

| Feature | Description |
|---|---|
| 8730-32D Platform | Extreme ONE OS version 22.2.0.0 supports 400G platform 8730-32D.<br>For more information, see Extreme 8730 Installation Guide. |
| Port Operations | Extreme ONE OS supports the following port operations:<br>• Link operations<br>• FEC and FEC Counters<br>• Port LED<br>• Link Fault Signaling<br>• FCS/CRC Errors<br>• Carrier transitions<br>• Traffic counters<br>• 4*100G breakout (See Supported Optics on page 16) |
| Management Interface | Extreme ONE OS supports management of the device through Inband and Out of Band interfaces using IPv4 and IPv6.<br>8730-32D - Dual Management OOB interfaces support:<br>• 1G & 10G SFP+<br>• DHCP v4 and v6 client<br>• Mgmt Port LED<br>• Statistics<br>• Disabling IP forwarding on OOB interface<br>• Support Multi-VLAN |

| Feature | Description |
|---|---|
| Image Management | Extreme ONE OS supports firmware upgrade/ install for the following components:<br>• System Firmware<br>• BMC firmware<br>• BIOS<br>• Firelight<br>• HWROT UC<br>• CPU CPLD<br>• Power CPLD<br>• Port 0 CPLD<br>• Port 1 CPLD<br>Supports full install through HTTP, HTTPs, SCP, SFTP, USB, local disk.<br>The firmware full install process involves removing all existing partitions while ensuring the preservation of the necessary SSH and certification files during the installation.<br>To remove management certificates during firmware installation, use the "no-preserve" argument from the Extreme ONE OS CLI. |
| Logging | Extreme ONE OS Logging Infra supports:<br>• Trace log<br>• Syslog<br>• Config<br>• Firmware<br>• Security<br>• Logging console<br>• Tech support |
| Rsyslog | Extreme ONE OS supports transmission of log event records to central log collection server using:<br>• Rsyslog with RELP/TCP/UDP (IPv4 and IPv6)<br>• Rsyslog with RELP+TLS (IPv4 and IPv6)<br>• Rsyslog with TCP+TLS (IPv4 andIPv6) |
| Key Health Indicators | Extreme ONE OS supports the following Key System Health indicators:<br>• FAN, PSU, PCI info<br>• Disk Space info<br>• Micro-service Health |

| Feature | Description |
|---|---|
| Event Monitoring and Threshold Notifications | Extreme ONE OS supports event monitoring and threshold notifications through gNMI, SNMP and RASlog for the following:<br>• CPU and Memory Threshold<br>• Fan and PSU failure/Recovery events<br>• MLAG Cluster events<br>• Maintenance Mode events<br>• BGP and BFD events<br>• Hardware resources - ACL, Layer 2, Layer 3 |
| Integrated Appliance Hosting (IAH) / Third-Party Virtual Machine Hosting | Extreme ONE OS supports IAH to deploy and manage virtual machines for the following:<br>• Generic Virtual Machine (VM)<br>• Multiple VM<br>• Multiple disk image formats (QCOW2, RAW, VMDK, OVA)<br>• Management port plugin to VM<br>• Insight/internal port plugin to VM in VTD mode for IP traffic. |
| Zero Touch Provisioning (ZTP) Support over OOB interface | Extreme ONE OS supports ZTP of the system through OOB IPv4 interface only to provision a device without any manual intervention and download required firmware and apply configurations. |
| User Management | Extreme ONE OS supports local user management with admin and user role<br>**Note:** Only one default admin user is pre-configured.<br>The following attributes are supported for local users (admin and user):<br>• User inactivity<br>• User locking and unlocking<br>• Password aging<br>• Strong password attributes<br>• Show users |
| Password Management | Extreme ONE OS supports Password Management to securely create, store, manage, and use passwords.<br>Password expiry alert is supported through global config of password max-age, user password expiry alert, and trap.<br>**Note:** Special characters, "?" and "\|" are not supported in passwords/secrets. |
| Configuration Audit support | Extreme ONS OS supports audit of all the configurations done through CLI and gNMI to track any provisioning modifications. |

| Feature | Description |
|---|---|
| File Management | Extreme ONE OS supports the following operations on Config files:<br>• Copy files to and from device<br>• Applying saved config/saving the running config<br>• List contents of a directory<br>• Export coredumps/techsupport |
| Clock, Time Zone, Network Time Protocol (NTP) | Extreme ONE OS supports setting of date, time, and time zone through Manual configuration or sync through NTP servers.<br>• Supports NTP IPv4 and IPv6 server<br>• Acts as NTP peers |
| DHCP and DNS Client | Extreme ONE OS supports DHCP (IPv4 and IPv6) and DNS (IPv4 and IPv6) clients on both Inband and OOB interfaces. |
| Authentication, Authorization, and Accounting (AAA) services | Extreme ONE OS supports Authentication, Authorization, and Accounting Services for both Inband and OOB access using:<br>• RADIUS<br>• TACACS+<br>• LDAP |
| Remote Access Protocols | Extreme ONE OS supports following protocols for accessing the device CLI terminal remotely:<br>• SSH (enabled by default)<br>• Telnet (disabled by default) |
| File Transfer Protocols | Extreme ONE OS supports the following file transfer protocols:<br>• SFTP<br>• SCP<br>• HTTP/HTTPS |
| Certificate management | Extreme ONE OS supports certificate management to import or export required certificates:<br>• show command for certificate display<br>• delete command for certificate cleanup of app and ca certificate<br>• certificate generate command for generation of the app certificate |
| Key Chain Management | Extreme ONE OS supports openconfig-keychain for keychain management infra for the backed protocol for authentication:<br>• Configure keychain<br>• Key-id<br>• Crypto algorithms |

| Feature | Description |
|---|---|
| Token Management | Extreme ONE OS supports token management for gNMI access.<br>• Access token validity - 24 hrs<br>• Refresh token validity - 30 days |
| TLS Protocols | Extreme ONS OS supports both TLS and mTLS protocols. |
| Simple Network Management Protocol (SNMP) | Extreme ONE OS supports SNMP v1, v2c and v3.<br>See Extreme ONE OS Switching v22.2.0.0 SNMP MIB Reference Guide for supported MIB, SNMP operations, and Trap details. |
| Link Layer Discovery Protocol (LLDP) | Extreme ONS OS supports LLDP for devices to advertise their identity, capabilities, and neighbors on a local network. |
| Link Aggregation Control Protocol (LACP) | Extreme ONE OS supports LACP to combine multiple physical links into a single logical link for increased bandwidth and redundancy. |
| Bridge Domain | Extreme ONS OS supports Layer 2 broadcast domain used in modern networking in following modes:<br>• VLAN mode: Tagged, Untagged and Untagged Strict<br>• Default mode: Tagged, Dual Tagged and Untagged Strict |
| Rapid MAC Detection | Extreme ONE OS supports Rapid MAC Move Detection used to monitor and respond to frequent changes in the location of a MAC address within a Layer 2 domain.<br>This behavior indicates issues such as network loops, misconfigured devices, or flapping links. |
| Resilient Hashing | Extreme ONE OS supports Resilient Hashing used in networking to minimize traffic disruption when the composition of a load-balanced group such as a Link Aggregation Group (LAG) or Equal-Cost Multi-Path (ECMP) change due to link or path failures. |
| Address Resolution and Discovery Protocols | Extreme ONE OS supports following the Address Resolution and Discovery Protocols:<br>• ARP (IPv4 address-to-MAC resolution)<br>• ND (IPv6 neighbor discovery, including address resolution, Router Advertisement, Router Solicitation)<br>• GARP (unsolicited ARP for announcement or conflict detection)<br>• DAD (part of ND, for duplicate address detection) |

| Feature | Description |
|---|---|
| Static Routing | Extreme ONE OS supports IPv4 and IPv6 static routing, enabling network administrators to configure routes as needed. |
| Access Control List (ACL) | Extreme ONE OS supports configuring following types of ACLs:<br>• Security ACL (controls which traffic is permitted or denied to pass through a device)<br>• Receive ACL (specifically filters traffic destined to the control plane of a network device). |
| Quality/Classification of Service (QoS/CoS) | Extreme ONE OS supports the following QoS/CoS features:<br>• L2 QoS - uses the Class of Service (CoS) field in the 802.1Q VLAN tag (3 bits)<br>• L3 QoS - uses the Differentiated Services Code Point (DSCP) field in the IP header (6 bits)<br>• CPU CoS - (prioritization of traffic destined to are processed by the control plane (CPU) |
| Border Gateway Protocol (BGP) | Extreme ONE OS supports the following BGP features:<br>• iBGP ( IPv4 and IPv6)<br>• eBGP ( IPv4 and IPv6)<br>• Two Bytes / Four Octet AS Number<br>• Address Family IPv4 / IPv6<br>• Peer Group<br>• Static Neighbors<br>• Listen Range<br>• MD5 Authentication [hash key size: 80]<br>• eBGP Multihop<br>• Fast-External Failover<br>• Route Origination:<br>◦ Redistribution<br>◦ Network<br>◦ Default-information<br>• Load Balancing or ECMP<br>• Route Reflection<br>• Peer Group<br>• Overriding Local-AS<br>• Multi-instance Support<br>• BGP Graceful Restart<br>• BGP Port [179] Protection<br>• BGP add-path ( Receive only) |
| BGP-Prefix Independent Convergence (BGP-PIC) | Extreme ONE OS supports BGP PIC, a fast reroute mechanism in BGP that enables sub-second convergence in the event of network failures, without needing to reprocess all BGP prefixes. |

| Feature | Description |
|---|---|
| BGP Route Policy | Extreme ONE OS supports Routing Policy, enabling users to control the flow of routing information. User-defined route policies determine which routes are accepted or advertised by dynamic routing protocols. |
| Bidirectional Forwarding Detection (BFD) | Extreme ONE OS supports BFD, enabling rapid fault detection between two routers or switches along a path.<br>BFD Protocol in Extreme ONE OS supports:<br>• Static route as client for IPv4 and IPv6<br>• BGP as client for IPv4 and IPv6<br>• Single hop and multi-hop |
| Static Anycast Gateway | Extreme ONE OS supports Static Anycast Gateway for both IPv4 and IPv6 used primarily in Layer 3 (L3) networks, to provide default gateway redundancy. |
| Multi-Chassis LAG | Extreme ONE OS supports MLAG allowing two physical switches to operate as a single logical switch for link aggregation purposes. |
| Maintenance Mode | Extreme ONE OS supports Maintenance Mode, designed for scenarios where a switch must undergo maintenance — such as during an image upgrade. When Maintenance Mode is enabled:<br>• The switch is isolated from all connected devices by disabling all front panel ports.<br>• Connected devices detect the link-down state and automatically reroute traffic to the peer MLAG node, ensuring minimal disruption. |
| Port Mirroring | Extreme ONE OS supports traffic mirroring, which duplicates traffic from a source interface to a mirror session.<br>• Mirroring is supported in both ingress and egress directions.<br>• Each mirror session is associated with one or more destination interfaces. |

The following features are available in demonstration mode as part of this release.

Note
Demonstration mode features provide beta access to selected functionality ahead of their full production release:

- Demonstration Mode features are intended for lab use only and must not be deployed in production environments.
- These features may include known issues or limitations beyond those documented here.
- Syntax, behavior, and functionality are subject to change as development progresses.

| Feature | Description |
|---|---|
| BGP-EVPN | BGP EVPN is a control plane protocol that enables scalable and efficient Layer 2 and Layer 3 virtual network services over IP networks using BGP.<br>BGP EVPN is widely used in data centers and service provider networks to support technologies such as VxLAN, offering benefits such as:<br>• MAC/IP address learning through control plane (not flooding)<br>• ARP/ND suppression<br>• Seamless integration of bridging and routing |
| L2/L3 ARP Suppression | ARP suppression in Layer 2/Layer 3 networks, particularly in EVPN-VXLAN environments, is a technique used to reduce broadcast traffic. It prevents unnecessary ARP (Address Resolution Protocol) requests for IPv4 and ND (Neighbor Discovery) requests for IPv6 from flooding the network. |
| Static VxLAN | Static VxLAN (Virtual Extensible LAN) refers to a VxLAN deployment where the VxLAN Tunnel Endpoints (VTEPs) and MAC-to-VTEP mappings are manually configured, rather than being dynamically learned through a control plane such as BGP EVPN. |

| Feature | Description |
|---|---|
| Static Route with next-hop as an Interface | In static routing, you can configure the next hop as an interface instead of an IP address. In this setup, the router forwards packets directly out of the specified interface without resolving the next-hop IP address. This approach works well for point-to-point links (e.g., serial or tunnel interfaces). However, on multi-access networks like Ethernet, it may cause issues if the router cannot determine the destination's MAC address. |
| Fabric Quality of Service (QoS) | Fabric QoS (Quality of Service) in data center or spine-leaf network architectures helps manage and prioritize traffic. Fabric QoS ensures consistent performance and reliability for critical applications by applying traffic handling policies across the fabric. |

## Hardware Support

Extreme ONE OS Switching supports the following device:

- 8730-32D

## Supported FEC Modes

| Port Type | Media Type | Default FEC Mode | Supported FEC Modes |
|---|---|---|---|
| 400G | 400G DR4 | RS-FEC | • Auto<br>• RS-EFC |
| 400G | 400G DAC | RS-FEC | • Auto<br>• RS-EFC |
| 400G | 400G SR8 | RS-FEC | • Auto<br>• RS-EFC |
| 400G | 400G LR4/LR4P | RS-FEC | • Auto<br>• RS-EFC |
| 400G | 400G AOC | RS-FEC | • Auto<br>• RS-EFC |
| 400G | 400G DR4X | RS-FEC | • Auto<br>• RS-EFC |
| 400G | 400G Fr4 | RS-FEC | • Auto<br>• RS-EFC |

| Port Type | Media Type | Default FEC Mode | Supported FEC Modes |
|---|---|---|---|
| 100G | 100G DAC | RS-FEC | • Auto<br>• RS-EFC<br>• Disabled |
| 100G | 100G SR4 | RS-FEC | • Auto<br>• RS-EFC<br>• Disabled |
| 100G | 100G Breakout Dr | Disabled | • Auto<br>• RS-EFC<br>• Disabled |
| 100G | 100G Breakout FR | Disabled | • Auto<br>• RS-EFC<br>• Disabled |

## Supported Optics

For a complete list of all supported optics, see Extreme Optics at https://optics.extremenetworks.com/ONE/

## Limitations and Restrictions

| Feature | Limitations and Restrictions |
|---|---|
| Firmware Upgrade - Full install mode support | When a firmware update is performed, the reboot reason code will display as "firmware update" instead of "full-install". |
| Resilient Hashing (RH) | RH does not support changes to ECMP paths made by routing protocols. If a protocol such as BGP updates ECMP paths, RH cannot maintain flow consistency. |
| BFD | The following features are not supported:<br>• Authentication<br>• Demand and Echo modes |
| MLAG cluster robustness | MLAG Resiliency is not supported for all the critical system error conditions. The known ones that are not handled are as follows<br>• QSFP I2C lock up detection logic<br>• BCM PCIe bus fault detection<br>• FAN failure detection<br>• PSU failure detection<br>• Thermal sensors failure detection<br>• BMC failure detection<br>• Disk failures detection |

| Feature | Limitations and Restrictions |
|---|---|
| BGP Events and Notifications | • Only IPv4 Standard MIB is supported<br>• Only IPv6 Enterprise MIB is supported |
| BFD Events and Notifications | • Standard MIB is not supported<br>• Only Enterprise MIB is supported along with proprietary Extreme MIB. |
| Maintenance Mode Notifications | During device reload, there is a delay of 60 seconds between trap event occurrence time and delivering these traps to recipient hosts. |
| L3 HW Resource Monitoring | • There is no alarm support.<br>• The configuration to rate-limit the generation of events and traps through threshold monitoring is currently not available.<br>• The snmpwalk for threshold monitor MIBs is not supported. |
| IPV6 RA RS | The following features are not supported:<br>• Origination of Router Solicitation<br>• IPV4 Router advertisement |
| List Key Values | Special characters such as @, #, $, *, [,] are not supported in list key values.<br>Key-values containing these special characters are not accepted. |
| SNMP | When snmpwalk is performed at the root, snmpwalk on all MIBs may end with the following message: "No more variables left in this MIB View (It is past the end of the MIB tree)". There are no issues when MIB OID is used for snmpwalk. |
| Static Routing | Proxy ARP/ND is not supported. |
| BGP Underlay | The following features are not supported:<br>• Confed-AS<br>• IPv6 Link-local Peering<br>• Selection-Knobs (Weight, Default-Metric, Enforce-First-AS)<br>• Route-Aggregation, Communities |
| CPU CoS | • When the protocol is disabled globally or interface level, the CPU CoS counters are still seen<br>• CLI support is limited to queue level counters |

| Feature | Limitations and Restrictions |
|---|---|
| L2 / L3 QoS | Due to a hardware limitation of only four multicast queues, counters for unknown unicast and multicast traffic are mapped accordingly.<br>• Updating the default-traffic-class value overwrites the CoS 0 to TC (Traffic Class) mapping in hardware for default mode BD (Bridge Domain) members.<br>• Egress L2 Remarking is always enabled in hardware.<br>• To apply ingress QoS maps on VLAN Mode BD, configure QoS Maps under the Ethernet or Port-Channel interface. This ensures the configuration is looped through all LIFs (Logical Interfaces) under the interface and applied consistently.<br>• Any QoS configuration applied directly to VLAN Mode BD LIFs is ignored. If the same LIF is moved to a Default Mode BD, the configuration is replayed.<br>• The Trust DSCP setting is not effective unless a user-defined map is configured and attached to the L2 LIF.<br>• If a specific QoS configuration exists on a LIF under an Ethernet or Port-Channel interface, the QoS Map from the parent interface is not applied until the specific configuration is removed from the LIF.<br>• When QoS configuration is deleted from a LIF, the configuration from the parent Ethernet or Port-Channel interface is automatically applied to the LIF. |
| GARP | Trailer bits are stripped off from GARP packets if suppress-arp and arp-snooping are enabled. |
| BGP Default route originate | Only the default-route-originate command method is supported on per peer-group.<br>The redistribute/send-default-route and network commands are globally supported and applicable to all peer-groups.<br>However, all three methods are not supported on a per peer-group basis. |
| Rapid Mac Move Detection | MAC move detection events in console are logged for only one interface if action is set to RASLOG when MAC move happens in multiple ports for the same MAC. |
| Authentication, Authorization and Accounting (AAA) | Radius accounting for GNMI is not supported. |

| Feature | Limitations and Restrictions |
|---|---|
| Logging | • All system logs such as /var/auth/log are by default exported to the syslog server<br>• Filtering is not supported<br>• Time zone changes will be effective after reload for timestamp change for the new trace logs of microservices. However, system clock is updated immediately |
| Certificate Management | Certificate import or export command displays password on screen in plain text. |
| Port Operations | Advanced port QSFP28, ToD, and GNSS port on 8730 platform are not supported. |
| OOB (Management port) | • If the secondary port is active and the primary port is down, replugging the primary port and removing the secondary within 5 seconds does not trigger a change in active mode.<br>• MTU settings are currently not supported for OOB management interfaces.<br>• On 8730 platform mgmt 0, interface operates at a fixed speed of 10G. When interface mgmt 0 is up or down, the individual speeds of mgmt 1 and mgmt 2 are reflected on respective interfaces, extMgmt 1 and extMgmt 2. |

## Open Issues

The following defects are open in this release of the software.

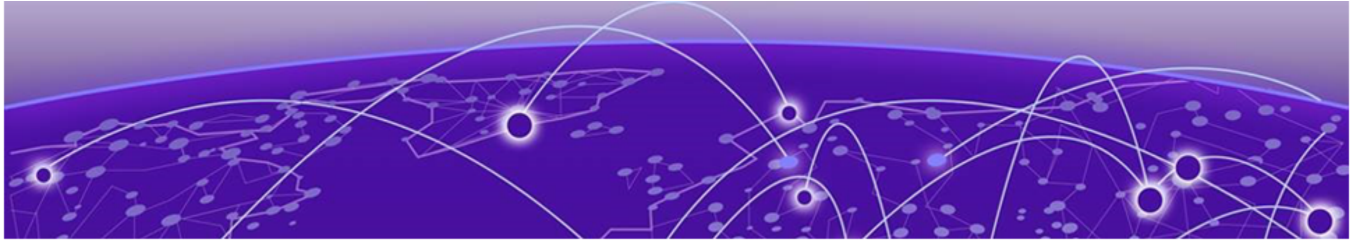
| Issue ID | Description |
|---|---|
| TOS-26768 | 'show system internal [cdb \|sdb]' commands render user provided secrets, needed for machine-to-machine communication, in plain text format |
| TOS-26852 | When services SSH, telnet, gRPC server, and NTP are enabled on 8730, a gNMI client subscribing to ON_CHANGE notification receive duplicate notifications from 8730 indicating that the service is enabled. |
| TOS-27020 | After logging into the CLI shell, configuration and execution commands function as expected; however, CLI help options `?` and tab do not work. Exit from the current CLI session and re-login. |
| TOS-28899 | Even without any actual data changes, streaming may still occur with on-change subscription enabled. |

| Issue ID | Description |
|---|---|
| TOS-29066 | After using the `certificate-manager import` command, the imported certificate may not appear in the `show certificate-manager` output.<br>If an invalid `source-ip` argument is provided, the operation fails without displaying an error message. |
| TOS-29080 | The device allows same static IP address configuration for both the Device Management port and for the TPVM management port, which may lead to communication issues between the two interfaces. |

## Acronyms and Abbreviations

| Term | Definition |
|---|---|
| AAA | Authentication Authorization and Accounting |
| ACL | Access Control List |
| ARP | Address Resolution Protocol |
| BFD | Bidirectional Forwarding Detection |
| BGP | Border Gateway Protocol |
| BIOS | Basic Input/Output System |
| BMC | Baseboard Management Controller |
| CoS | Classification of Service |
| DAD | Duplicate Address Detection |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| ECMP | Equal-Cost Multi-Path |
| EVPN | Ethernet Virtual Private Network |
| GARP | Gratuitous Address Resolution Protocol |
| gNMI | gRPC Network Management Interface |
| HWROT | Hardware Root of Trust |
| IAH | Integrated Application Hosting |
| LACP | Link Aggregation Control Protocol |
| LAG | Link Aggregation Group |
| LFS | Link Fault Signaling |
| LLDP | Link Layer Discovery Protocol |
| MIB | Management Information Base |
| MLAG | Multi-Chassis LAG |

| Term | Definition |
|---|---|
| mTLS | Mutual Transport Layer Security |
| ND | Neighbor Discovery |
| NTP | Network Time Protocol |
| OOB | Out of Band |
| OOM | Out of Memory |
| PIC | Prefix Independent Convergence |
| QoS | Quality of Service |
| RADIUS | Remote Authentication Dial-In User Service |
| SNMP | Simple Network Management Protocol |
| TACACS | Terminal Access Controller Access Control System |
| TLS | Transport Layer Security |
| VxLAN | Virtual Extensible LAN |
| VLAN | Virtual Local Area Network |
| ZTP | Zero Touch Provisioning |



# Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

## Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.

3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.