Extreme ONE OS Switching v22.2.1.0 Release Notes

New Features, Bug Fixes, and Known Limitations

9039424-00 Rev AA
December 2025

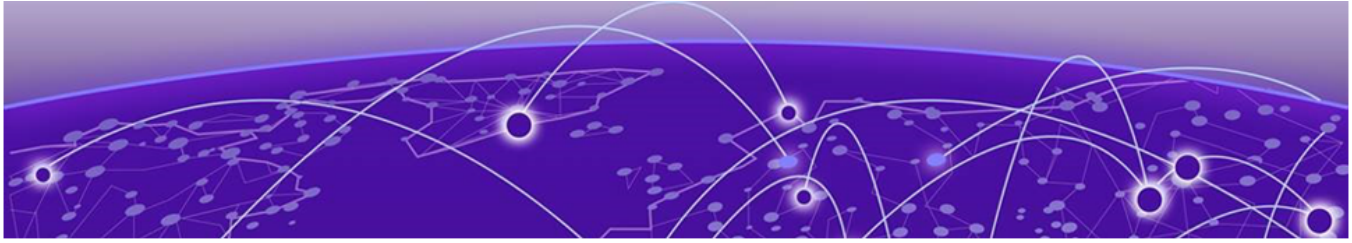
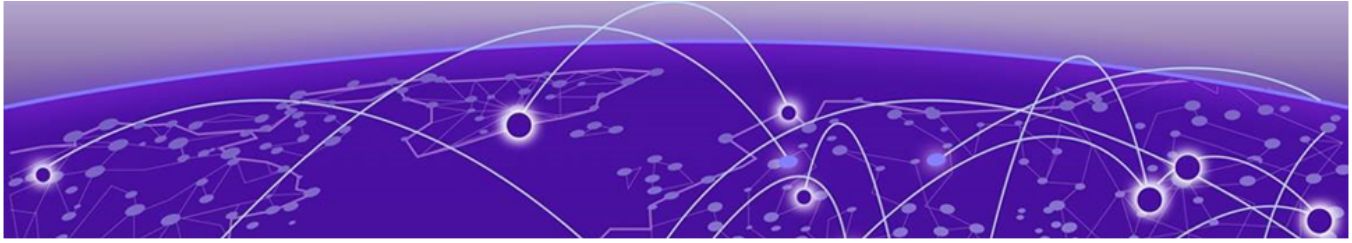


Table of Contents



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

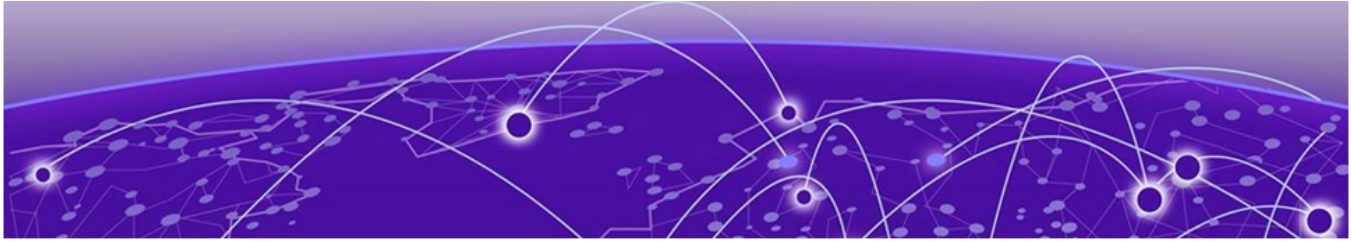
Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

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

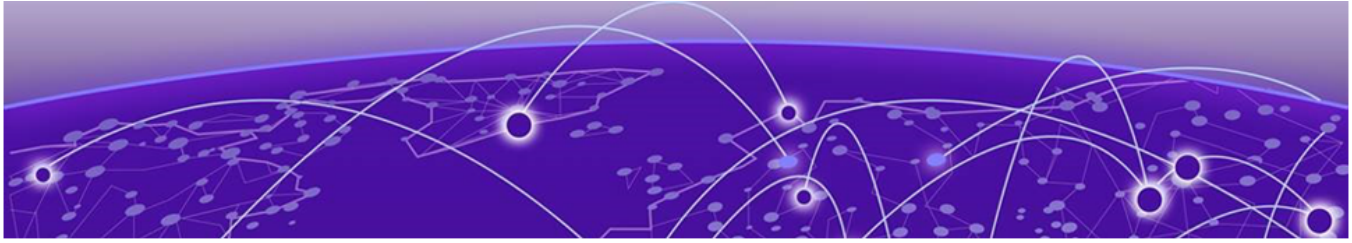
Open Source Declarations

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

The Extreme ONE OS Switching v22.2.1.0 Release Notes provides a comprehensive overview of essential updates, technical improvements, and known limitations for advanced IP fabric and data center environments. It highlights enhancements in configuration recovery, security, management interfaces, and network resiliency, with expanded protocol and hardware support. The document provides guidance on deployment scenarios, configuration best practices, and troubleshooting, addressing open issues and restrictions relevant to network engineers and administrators.



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 devices.

New in this Release

Extreme ONE OS Switching 22.2.1.0 introduces the following features and enhancements.

Feature	Supported Platform	Description
Startup-config / backup-config Support	All platforms	The Backup Configuration feature ensures that device can recover its configuration in two key scenarios: • Automatic recovery on config-db corruption • Apply backup-config on immediate reboot
License Management (Advanced Core)	8730-32D	The ADVANCED_CORE license is applicable only on the 8730 platform. This EULA covers the IAH feature on 8730 platform.
License Management (Advanced Features)	All platforms	Except for 8730, this EULA includes IAH and BGP-EVPN features on all Extreme ONE OS Switching platforms. For 8730, it covers only BGP-EVPN.
min TLS Support	All platforms	Supports minimum TLS version configuration on TLS-enabled services. This includes client services such as LDAP, RADIUS, Syslog, and HTTPS, as well as the gRPC server.
Ethernet Link Error Disable (Basic Link Dampening)	All platforms	Ethernet Link Error Disable helps mitigate instability by temporarily delaying or suppressing link state changes. Dampening with the link set to admin down helps prevent issues caused by rapidly flapping interfaces.
SNMP Get & GetNext for Monitoring	All platforms	Supports SNMP Get and GetNext for the following with the existing SNMP trap support: • Threshold Monitoring • Temperature Sensor
Egress Port Scheduler	8730-32D	Prioritizes and schedules packet transmission at egress ports, ensuring optimal network performance and traffic flow management.
MLAG Resiliency	All platforms	Enhances MLAG resiliency by preventing split-brain mode when ISL shuts down before Keep-Alive signals. This improvement maintains acceptable convergence times and minimizes traffic disruption during system fault events.
Fabric QoS	All platforms	Defines rules for deriving the internal traffic class of a packet based on its content and user configuration. On egress, applies rules for remarking QoS-related fields such as VLAN PCP and IP DSCP/ToS byte.

Feature	Supported Platform	Description
BGP IPv6 Prefix Advertisement over IPv4 BGP Peers	All platforms	Enables IPv6 routing information exchange over existing IPv4 BGP sessions using Multiprotocol BGP (MP-BGP), eliminating the need for separate IPv6 BGP sessions.
Static Routes with Interface-Based Next Hop	All platforms	Supports manual configuration of static IPv4 and IPv6 routes with next-hop functionality for IP addresses and interfaces, including Ethernet, Port Channel (PO), and Virtual Ethernet (VE).

Hardware Support

Extreme ONE OS Switching 22.2.1.0 supports Extreme 8520, Extreme 8720, Extreme 8730, and Extreme 8820 hardware platforms.

Supported FEC Modes

Table 1: Extreme 8730 FEC Matrix

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
400G	400G DR4	RS-FEC	• Auto • RS-FEC
400G	400G DAC	RS-FEC	• Auto • RS-FEC
400G	400G SR8	RS-FEC	• Auto • RS-FEC
400G	400G LR4	RS-FEC	• Auto • RS-FEC
400G	400G LR4P	RS-FEC	• Auto • RS-FEC
400G	400G AOC	RS-FEC	• Auto • RS-FEC
400G	400G DR4X	RS-FEC	• Auto • RS-FEC
400G	400G Fr4	RS-FEC	• Auto • RS-FEC
100G	100G DAC	RS-FEC	• Auto • RS-FEC • Disabled

Table 1: Extreme 8730 FEC Matrix (continued)

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
100G	100G SR4	RS-FEC	• Auto • RS-FEC • Disabled
100G	100G eSR4	RS-FEC	• Auto • RS-FEC • Disabled
100G	100G 4WDM	Disabled	• Auto • RS-FEC • Disabled
100G	100G CWDM	RS-FEC	• Auto • RS-FEC • Disabled
100G	100G SWDM4	Disabled	• Auto • RS-FEC • Disabled
100G	100G Dr	Disabled	• Auto • RS-FEC • Disabled
100G	100G FR	Disabled	• Auto • RS-FEC • Disabled
100G	100G AOC	RS-FEC	• Auto • RS-FEC • Disabled
100G	100G LR4	Disabled	• Auto • RS-FEC • Disabled
100G	100G LR4-Lite	RS-FEC	• Auto • RS-FEC • Disabled
100G	100G ER4LT	Disabled	• Auto • RS-FEC • Disabled
100G	100G Breakout Dr	Disabled	• Auto • RS-FEC • Disabled

Table 1: Extreme 8730 FEC Matrix (continued)

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
100G	100G Breakout FR	Disabled	• Auto • RS-FEC • Disabled
100G	100G Breakout LR	Disabled	• Auto • RS-FEC • Disabled
25G	Breakout DAC	RS-FEC	• Auto • RS-FEC • FC-FEC • Disabled
25G	Breakout SR	Disabled	• Auto • RS-FEC • FC-FEC • Disabled
25G	Breakout AOC	Disabled	• Auto • RS-FEC • FC-FEC • Disabled
25G	25G LR	Disabled	• Auto • RS-FEC • FC-FEC • Disabled

Table 2: Extreme 8720, Extreme 8520, and Extreme 8820 FEC Matrix

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
100G	100G DAC	RS-FEC	• Auto • RS-FEC • Disabled
100G	100G SR4	RS-FEC	• Auto • RS-FEC • Disabled
100G	100G eSR4	RS-FEC	• Auto • RS-FEC • Disabled

Table 2: Extreme 8720, Extreme 8520, and Extreme 8820 FEC Matrix (continued)

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
100G	100G 4WDM	Disabled	• Auto • RS-FEC • Disabled
100G	100G CWDM	RS-FEC	• Auto • RS-FEC • Disabled
100G	100G SWDM4	Disabled	• Auto • RS-FEC • Disabled
100G	100G Dr	Disabled	• Auto • RS-FEC • Disabled
100G	100G FR	Disabled	• Auto • RS-FEC • Disabled
100G	100G AOC	RS-FEC	• Auto • RS-FEC • Disabled
100G	100G LR4	Disabled	• Auto • RS-FEC • Disabled
100G	100G LR4-Lite	RS-FEC	• Auto • RS-FEC • Disabled
100G	100G ER4LT	Disabled	• Auto • RS-FEC • Disabled
100G	100G Breakout FR	Disabled	• Auto • RS-FEC • Disabled
25G	Breakout DAC	RS-FEC	• Auto • RS-FEC • FC-FEC • Disabled

Table 2: Extreme 8720, Extreme 8520, and Extreme 8820 FEC Matrix (continued)

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
25G	Breakout SR4	Disabled	• Auto • RS-FEC • FC-FEC • Disabled
25G	Breakout AOC	Disabled	• Auto • RS-FEC • FC-FEC • Disabled
25G	25G LR	Disabled	• Auto • RS-FEC • FC-FEC • 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
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: • Authentication • Demand and Echo modes
BGP Events and Notifications	• Only IPv4 Standard MIB is supported • Only IPv6 Enterprise MIB is supported
BFD Events and Notifications	• Standard MIB is not supported • 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.

Feature	Limitations and Restrictions
L3 HW Resource Monitoring	• There is no alarm support. • The configuration to rate-limit the generation of events and traps through threshold monitoring is currently not available. • The snmpwalk for threshold monitor MIBs is not supported.
IPV6 RA RS	The following features are not supported: • Origination of Router Solicitation • IPV4 Router advertisement
List Key Values	Special characters such as @, #, $, *, [,] are not supported in list key values. 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: • Confed-AS • IPv6 Link-local Peering • Selection-Knobs (Weight, Default-Metric, Enforce-First-AS) • Route-Aggregation, Communities
CPU CoS	• When the protocol is disabled globally or interface level, the CPU CoS counters are still seen • 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. • Updating the default-traffic-class value overwrites the CoS 0 to TC (Traffic Class) mapping in hardware for default mode BD (Bridge Domain) members. • Egress L2 Remarking is always enabled in hardware. • 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. • 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. • The Trust DSCP setting is not effective unless a user-defined map is configured and attached to the L2 LIF. • 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. • 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. The redistribute/send-default-route and network commands are globally supported and applicable to all peer-groups. 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. • Filtering is not supported. • Time zone changes will be effective after reload for timestamp change for the new trace logs of microservices. However, system clock is updated immediately. • Forward Referencing to tls-profile-id is not supported: **Workaround:** 1. Import required ca certificate before configuring rsyslog server. 2. If rsyslog is already configured and a CA certificate is imported or rotated later, delete the `tls-profile-id` in the rsyslog configuration and reconfigure it. • Relp or relp+tls is not supported over inband.
Certificate Management	When using the certificate import or export command, if the password is provided inline, it is displayed in plain text on the screen. **Workaround:** As a workaround, use the interactive method to import or export the certificate. In this mode, the password is entered securely and is not displayed on the screen.
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. • MTU settings are currently not supported for OOB management interfaces. • 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-31572	Traffic is not load balanced after changing load balancing headers. **Symptom:** Load balancing for certain fields does not work, except for specific fields in TD4. **Condition:** Only specific fields are supported: • Ethernet: Load balancing works only on `dst-mac`. • IPv4 and IPv6: Load balancing works only on `dst-ip`. **Workaround:** Enable the default load balancing configuration.
TOS-31422	All MLAG and uplink interfaces on the secondary MLAG peer may flap momentarily when the primary peer experiences an Out-of-Memory (OOM) condition. **Symptom:** All MLAG/Uplink interfaces on the secondary MLAG peer may flap momentarily. **Condition:** This occurs when the primary MLAG peer reboots due to an Out-of-Memory condition. **Recovery:** Interfaces automatically recover without any manual intervention.
TOS-31353	`gNOI rpc` for system programmable update fails with unauthorized access. **Symptom:** The GNOI RPC APIs for low-level firmware upgrades do not function properly, whereas the CLI commands for the same operation work as expected. **Condition:** This issue occurs during upgrades of low-level firmware components such as BMC and CPLD. **Workaround:** Use CLI commands to perform these low-level firmware upgrades.

Issue ID	Description
TOS-31295	After an uncontrolled restart of UFTM, some BFD sessions restart. **Symptom:** Some BFD sessions configured for static routes flap. **Condition:** This occurs when the UFTM microservice crashes due to software exceptions. **Recovery:** Sessions automatically come up after going down; no manual intervention is needed.
TOS-31287	Intermittent Layer 3 north–south traffic drops are observed after upgrading devices. **Symptom:** In a scaled environment, intermittent traffic drops may occur momentarily on a few streams when the primary MLAG node is rebooted. **Condition:** This issue occurs on MLAG setups during a primary MLAG node reboot. **Workaround:** • Perform a `shut`/`no shut` on the affected interface where packet drops are observed. • Alternatively, `clear IP routes` for the impacted VRF.
TOS-31015	LACP Port-Channel interfaces may flap for a few seconds after running the command **`iah vm import TPVM tpvm disk://iah/tpvm-4.7.9-3.amd64.deb`**. **Symptom:** On 8720-32C devices in scaled environments, when executing **`IAH TPVM Import`**. LACP POs go down and recover only after the import completes due to CPU resource limitations.
TOS-30644	`show qos counters` for unit1 Ports always gives zero values. **Symptom:** QoS per-queue counters are not available for ports Ethernet 0/41–80 on 8820-80C platforms. **Condition:** On these platforms, the command **`show counters qos interface ethernet 0/X queue all`** does not display counters for unit-1 interfaces (Ethernet 0/41–80).
TOS-29497	Error message `systemd-journald[3922]: Failed to create new system journal: No such file or directory` may appear after upgrading the device to the latest image. **Symptom:** During device reboot, `systemd-journald` error logs may appear: **Condition:** This occurs only on the first boot after the system is updated.

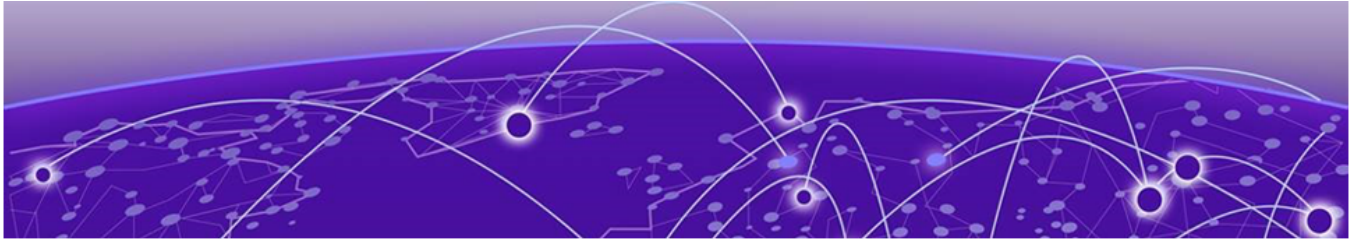
Issue ID	Description
TOS-28935	Ingress traffic with an MPLS GRE header is dropped on TD3 platforms. **Symptom:** MPLS traffic over GRE tunnels is dropped at the hardware layer. **Condition:** This issue occurs for MPLS-over-GRE traffic received on default-mode bridge domains (BD).
TOS-27021	SSH access to the CLI terminal is slower than expected. **Symptom:** After logging into a ONE OS device, the CLI prompt takes longer than expected to appear.
TOS-25000	Error message `Write failed` may appear while the device is coming up after a reload. **Symptom:** Write operations to the Port CPLD fail intermittently, which may cause front-panel LEDs to turn off. **Condition:** Due to CPLD instability, write operations to CPLD registers that enable LED power sometimes fail. **Recovery:** Reloading the device resolves the issue.

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
CLI	Command Line Interface
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

Term	Definition
FEC	Forward Error Correction
GARP	Gratuitous Address Resolution Protocol
GRUB	GRand Unified Bootloader
gNMI	gRPC Network Management Interface
HTTP	HyperText Transfer Protocol
HWROT	Hardware Root of Trust
IAH	Integrated Application Hosting
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LED	Light Emitting Diode
LFS	Link Fault Signaling
LLDP	Link Layer Discovery Protocol
MIB	Management Information Base
MLAG	Multi-Chassis LAG
mTLS	Mutual Transport Layer Security
ND	Neighbor Discovery
NTP	Network Time Protocol
ONIE	Open Network Install Environment
OOB	Out of Band
OOBM	Out-of-Band Management
OOM	Out of Memory
PIC	Prefix Independent Convergence
PSU	Power Supply Unit
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RME	Redundant Management Ethernet
SCP	Secure Copy Protocol
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TACACS	Terminal Access Controller Access Control System
TPVM	Third-Party Virtual Machine
TLS	Transport Layer Security
USB	Universal Serial Bus
VxLAN	Virtual Extensible LAN

Term	Definition
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.