

Customer Release Notes

Fabric Engine

Software Release 9.4.2.0

October 2026

INTRODUCTION:

This document describes important information about this release for platforms that support Extreme Networks Fabric Engine™.

The purpose of this version is to address customer and internally found software issues.

Newly Purchased Switches Require Software Upgrade. You should promptly upgrade the Fabric Engine software to the latest version available by visiting the Extreme Portal.

Extreme Networks recommends that you thoroughly review this document prior to installing or upgrading this product.

For the latest firmware versions, visit the download site at:
www.extremenetworks.com/support/

NEW IN THIS RELEASE:

Hardware:

- 7830 – New qualified 400G cables

Software:

- EDM shows same licensing info as CLI
- License expiry log messages for EP1/Pilot licenses about to expire
- Update time-zone information for UTC changes in Alberta & British Columbia (Canada)

NOS-APIs:

- Removal of premier license requirement
- Support for user certificates and SCEP support

Security improvements for FIPS 140-3

IMPORTANT NOTES BEFORE UPGRADING TO THIS RELEASE:

Please see “Fabric Engine Release Notes for version 9.4.0.0” available at
<https://www.extremenetworks.com/support/release-notes>

UPGRADE CONSIDERATIONS WHEN UPGRADING TO 9.4.2.0 FROM PREVIOUS RELEASES:

Please see “Fabric Engine Release Notes for version 9.4.0.0” available at
<https://www.extremenetworks.com/support/release-notes>

This release contains a corrected OSPF HMAC-SHA (SHA-1 and SHA-256) hash calculation that fixes interoperability with other vendors but is not backward compatible with previous Fabric Engine releases (VOSS-35194).

Before upgrade, the OSPF authentication should be disabled on OSPF adjacencies to avoid extended OSPF routing interruption and re-enabled after both OSPF peers are upgraded to 9.4.1.0 or newer.

PLATFORMS SUPPORTED:

Please see "Fabric Engine Release Notes for version 9.4.0.0" available at <https://www.extremenetworks.com/support/release-notes> for details regarding supported platforms.

FILE NAMES FOR THIS RELEASE:

Extreme Switching 4220 Series

File Name	Module or File Type	File Size (bytes)
4220.9.4.2.0_edoc.tar	Logs Reference	40110080
4220.9.4.2.0.md5	MD5 Checksums	521
4220.9.4.2.0_mib_sup.txt	MIB - supported object names	1462842
4220.9.4.2.0_mib.txt	MIB - objects in the OID compile order	8732578
4220.9.4.2.0_mib.zip	Archive of all MIB files	1294139
4220.9.4.2.0_oss-notice.html	Open-source software - Master copyright file	2597473
4220.9.4.2.0.sha512	SHA512 Checksums	1532
4220.9.4.2.0.voss	Software image	112306020
dictionary.fabricengine	RADIUS dictionary	3502
FabricEnginev9.4.0_HELP_EDM_gzip.zip	EDM Help file	5323371
restconf_yang.tgz	YANG model	506020

Extreme Switching 5320 Series

File Name	Module or File Type	File Size (bytes)
5320.9.4.2.0_edoc.tar	Logs Reference	40120320
5320.9.4.2.0.md5	MD5 Checksums	521
5320.9.4.2.0_mib_sup.txt	MIB - supported object names	1587149
5320.9.4.2.0_mib.txt	MIB - objects in the OID compile order	8732578
5320.9.4.2.0_mib.zip	Archive of all MIB files	1294139
5320.9.4.2.0_oss-notice.html	Open-source software - Master copyright file	2597473
5320.9.4.2.0.sha512	SHA512 Checksums	1532
5320.9.4.2.0.voss	Software image	114597906
dictionary.fabricengine	RADIUS dictionary	3502
FabricEnginev9.4.0_HELP_EDM_gzip.zip	EDM Help file	5323371
restconf_yang.tgz	YANG model	506020

Extreme Switching 5420 Series

File Name	Module or File Type	File Size (bytes)
5420.9.4.2.0_edoc.tar	Logs Reference	40120320
5420.9.4.2.0.md5	MD5 Checksums	521
5420.9.4.2.0_mib_sup.txt	MIB - supported object names	1586915
5420.9.4.2.0_mib.txt	MIB - objects in the OID compile order	8732578
5420.9.4.2.0_mib.zip	Archive of all MIB files	1294139
5420.9.4.2.0_oss-notice.html	Open-source software - Master copyright file	2597473
5420.9.4.2.0.sha512	SHA512 Checksums	1532
5420.9.4.2.0.voss	Software image	114337435
dictionary.fabricengine	RADIUS dictionary	3502
FabricEnginev9.4.0_HELP_EDM_gzip.zip	EDM Help file	5323371
restconf_yang.tgz	YANG model	506020

Extreme Switching 5520 Series

File Name	Module or File Type	File Size (bytes)
5520.9.4.2.0_edoc.tar	Logs Reference	40120320
5520.9.4.2.0.md5	MD5 Checksums	521
5520.9.4.2.0_mib_sup.txt	MIB - supported object names	1585750
5520.9.4.2.0_mib.txt	MIB - objects in the OID compile order	8732578
5520.9.4.2.0_mib.zip	Archive of all MIB files	1294139
5520.9.4.2.0_oss-notice.html	Open-source software - Master copyright file	2597473
5520.9.4.2.0.sha512	SHA512 Checksums	1532
5520.9.4.2.0.voss	Software image	129590872
dictionary.fabricengine	RADIUS dictionary	3502
FabricEnginev9.4.0_HELP_EDM_gzip.zip	EDM Help file	5323371
restconf_yang.tgz	YANG model	506020

Extreme Switching 5720 Series

File Name	Module or File Type	File Size (bytes)
5720.9.4.2.0_edoc.tar	Logs Reference	40120320
5720.9.4.2.0.md5	MD5 Checksums	655
5720.9.4.2.0_mib_sup.txt	MIB - supported object names	1592621
5720.9.4.2.0_mib.txt	MIB - objects in the OID compile order	8732578
5720.9.4.2.0_mib.zip	Archive of all MIB files	1294139
5720.9.4.2.0_oss-notice.html	Open-source software - Master copyright file	2597473
5720.9.4.2.0.sha512	SHA512 Checksums	1858

File Name	Module or File Type	File Size (bytes)
5720.9.4.2.0.voss	Software image	330042893
dictionary.fabricengine	RADIUS dictionary	3502
FabricEnginev9.4.0_HELP_EDM_gzip.zip	EDM Help file	5323371
FabricIPSecGW_VM_5.2.0.0.ova	Fabric IPSec Gateway Virtual Machine	4034211840
restconf_yang.tgz	YANG model	506020
TPVM_Ubuntu24.04_04_03June2026.qcow2	Third Party Virtual Machine (TPVM)	3747785216

Extreme Switching 7520 Series

File Name	Module or File Type	File Size (bytes)
7520.9.4.2.0_edoc.tar	Logs Reference	40120320
7520.9.4.2.0.md5	MD5 Checksums	655
7520.9.4.2.0_mib_sup.txt	MIB - supported object names	1588419
7520.9.4.2.0_mib.txt	MIB - objects in the OID compile order	8732578
7520.9.4.2.0_mib.zip	Archive of all MIB files	1294139
7520.9.4.2.0_oss-notice.html	Open-source software - Master copyright file	2597473
7520.9.4.2.0.sha512	SHA512 Checksums	1858
7520.9.4.2.0.voss	Software image	330333145
dictionary.fabricengine	RADIUS dictionary	3502
FabricEnginev9.4.0_HELP_EDM_gzip.zip	EDM Help file	5323371
FabricIPSecGW_VM_5.2.0.0.ova	Fabric IPSec Gateway Virtual Machine	4034211840
restconf_yang.tgz	YANG model	506020
TPVM_Ubuntu24.04_04_03June2026.qcow2	Third Party Virtual Machine (TPVM)	3747785216

Extreme Switching 7720 Series

File Name	Module or File Type	File Size (bytes)
7720.9.4.2.0_edoc.tar	Logs Reference	40120320
7720.9.4.2.0.md5	MD5 Checksums	655
7720.9.4.2.0_mib_sup.txt	MIB - supported object names	1586606
7720.9.4.2.0_mib.txt	MIB - objects in the OID compile order	8732578
7720.9.4.2.0_mib.zip	Archive of all MIB files	1294139
7720.9.4.2.0_oss-notice.html	Open-source software - Master copyright file	2597473
7720.9.4.2.0.sha512	SHA512 Checksums	1858
7720.9.4.2.0.voss	Software image	330334527
dictionary.fabricengine	RADIUS dictionary	3502
FabricEnginev9.4.0_HELP_EDM_gzip.zip	EDM Help file	5323371

File Name	Module or File Type	File Size (bytes)
FabricIPSecGW_VM_5.2.0.0.ova	Fabric IPSec Gateway Virtual Machine	4034211840
restconf_yang.tgz	YANG model	506020
TPVM_Ubuntu24.04_04_03June2026.qcow2	Third Party Virtual Machine (TPVM)	3747785216

Extreme Switching 7830 Series

File Name	Module or File Type	File Size (bytes)
7830.9.4.2.0_edoc.tar	Logs Reference	40110080
7830.9.4.2.0.md5	MD5 Checksums	521
7830.9.4.2.0_mib_sup.txt	MIB - supported object names	1579420
7830.9.4.2.0_mib.txt	MIB - objects in the OID compile order	8732578
7830.9.4.2.0_mib.zip	Archive of all MIB files	1294139
7830.9.4.2.0_oss-notice.html	Open-source software - Master copyright file	2597473
7830.9.4.2.0.sha512	SHA512 Checksums	1532
7830.9.4.2.0.voss	Software image	460022992
dictionary.fabricengine	RADIUS dictionary	3502
FabricEnginev9.4.0_HELP_EDM_gzip.zip	EDM Help file	5323371
restconf_yang.tgz	YANG model	506020

Note about image download:

Ensure images are downloaded using the binary file transfer. Perform MD5 checksum check on downloaded files to ensure file integrity.

Check that the file type suffix is “.tgz” and the image names after download to device match those shown in the above table. Some download utilities have been observed to append “.tar” to the file name or change the filename extension from “.tgz” to “.tar”. If file type suffix is “.tar” or file name does not exactly match the names shown in above table, rename the downloaded file to the name shown in the table above so that the activation procedures will operate properly.

Load activation procedures:

```
software add 7720.9.4.2.0.voss
software activate 9.4.2.0.GA
```

or

```
software add 7520.9.4.2.0.voss
software activate 9.4.2.0.GA
```

or

```
software add 5720.9.4.2.0.voss
software activate 9.4.2.0.GA
```

or

```
software add 5520.9.4.2.0.voss
software activate 9.4.2.0.GA
```

or

```
software add 5420.9.4.2.0.voss
software activate 9.4.2.0.GA
```

or

```
software add 5320.9.4.2.0.voss
software activate 9.4.2.0.GA
```

or

```
software add 4220.9.4.2.0.voss
software activate 9.4.2.0.GA
```

or

```
software add 7830.9.4.2.0.voss
software activate 9.4.2.0.GA
```

CHANGES IN THIS RELEASE:

New Features in This Release

For the 7830 platform, support has been added for the following 400G cables:

- Siemon 400G-DACP-QSFPDD1M (VOSS-35396)
- Siemon 400G-DACP-QSFPDD2M (VOSS-35397)
- Siemon 400G-DACP-QSFPDD2Z5M (VOSS-35398)
- Siemon 400G-DACP-QSFPDD3M (VOSS-35399)

Software:

- **EDM shows same licensing info as CLI (VOSS-34934)**
- **License expiry log messages for EP1/Pilot licenses about to expire (VOSS-35482)**
 - Updated expiry log:
 - *1 2026-09-18T11:51:53.656Z 7520-48Y-8C-FabricEngine CPI - 0x000000712 - 00000000 GlobalRouter SW INFO License check of product STANDARD failed, license assignment will expire in 2 day(s)*
- **Update time-zone information for UTC changes in Alberta & British Columbia (Canada) (VOSS-35545)**

NOS-APIs:

- **Removal of premier license requirement for OpenAPI (VOSS-35516)**
- **Support for user certificates and SCEP support (VOSS-34920)**
A new CLI command is now available to add a certificate for OpenAPI:
VOSS:1(config)#application
VOSS:1(config-app)# openapi local-mgmt certificate ca-common-name WORD<1-45>

Added extra output to ***"show application openapi"*** command for certificate details:

```
=====
OpenAPI Info
=====
```

```
Server State           : Disabled
Server Operational State : Not Running
Server State Local Port : Disabled
Local Port State       : Disabled
Local TCP Port          : 9443
TLS                     : Enabled
TLS version             : 1.2
TTL(in seconds)         : 86400
Certificate CA Common Name : N/A
Certificate Type         : Self-Signed
Server Version          : 0.1.15.8
Specification Version    : N/A
```

Security improvements for FIPS 140-3:

- FIPS 186-5 RSA support has been added
- MACsec self-test at boot time (Encrypted Packet Match) has been implemented for 5520, 5720 and 7520 MACsec capable models
- File size for boot image file is compared to their counterparts in /intflash/releases and an error is returned in case of mismatch
- Zeroization for sensitive files now shows Log Reports when started and completed

Old Features Removed From This Release

None

Problems Resolved in This Release

VOSS-35436	After a vIST switch recovers after a reboot, connected devices in SMLT can lose connectivity to the uplink devices.
CFD-13433	RESTCONF TACACS+ authentication fails intermittently after extended uptime, requiring the RESTCONF application to be restarted.
CFD-13433	RESTCONF TACACS+ authentication fails intermittently after extended uptime, requiring the RESTCONF application to be restarted.
CFD-15790	BFD sessions to all neighbors flap simultaneously on random switches and take about 6 seconds to reestablish, without a corresponding interface flap or CPU queue drop.
VOSS-34983	On the 5520-24X, 1G fiber SFP links with auto-negotiation enabled fail to establish after upgrading from 9.2.2.0 to 9.3.3.0/9.4.1.0, with the remote side showing the link as down.
CFD-16785	SCP and SFTP file transfers hang on some nodes while SSH continues to work, eventually exhausting the maximum session count and blocking further file transfers.
CFD-16890	NEAP-LLDP authenticated sessions are not cleared when the connected IP phone is physically disconnected from the port. The stale session persists until LLDP timeout, preventing new devices from authenticating with a "Maximum allowed MAC reached" error.
CFD-17112	MACsec MKA-secured links flap intermittently on 7520-48YE-8CE switches
CFD-17133	SNMP requests over the management VLAN remain unanswered due to incorrect routing of management traffic.
CFD-17203	Disabling ISIS in a particular EAP related scenario may cause the switch to generate a core dump and reboot.
CFD-17320	Ping response times through VLAN or CLIP interfaces show intermittent latency spikes of several hundred milliseconds after a switch is onboarded to XIQ/Platform One.

Problems Resolved in This Release	
CFD-17400	Core switches repeatedly log 'tMAIN latency is HIGH' warnings tied to smltTick delays, coinciding with customer reports of network slowness.
CFD-17507	When an IGMPv3 receiver joins a multicast group using INCLUDE-source mode with the source list configured as "any source", and a local multicast sender transmits to the same group using source IP address 0.0.0.0, the switch becomes unresponsive and eventually reboots.
CFD-17511	A switch may unexpectedly reboot due to a code flaw in internal mutex handling.
CFD-17575	After an upgrade, the switch repeatedly logs 'EdmPost(): Out-Of-Memory - EdmEnvoyCookie too big' errors to the console, and SSH/web access can become unavailable.
CFD-17608	When NEAP client switches to EAP, the port ACL table displays a generic implicit name such as 'EAP-MHNV-<port>' instead of the manually configured ACL name for some dynamic RADIUS-based ACL sessions.
CFD-17633	DHCP snooping bindings are lost when the RADIUS server becomes unreachable and are not repopulated once the RADIUS server becomes reachable again, in a fail-open-ISID configuration.
CFD-17646	With MC Lite and IGMP v3 configured, the switch sends group-specific multicast queries with an all-zero source address instead of the configured querier address, and multicast traffic can stop reaching non-responding clients.
VOSS-35417	Entering incorrect EAP credentials during authentication leaves stale EAP/NEAP sessions for the same MAC address, eventually causing the switch to reach its MAC limit and drop the client.
CFD-17672	The switch periodically logs a 'dpmGetIngressPortRateLimitStats: ltrSend FAILED' error once or twice a day with no observed network impact.
CFD-17686	The switch unexpectedly crashed when processing a BGP route update.
CFD-17728	A switch crashed with a "tMainTask, signal 6" error shortly after a device authenticated on a port that had been flapping.
CFD-17744	The DHCP server process crashes and stops leasing addresses when both a TFTP server list (option 150) and a domain name are configured together in a DHCP pool.
CFD-17831	Running 'show isis spbm unicast-tree' over SSH caused an unexpected reboot with a core file.
CFD-17863	An untagged EAP 'Success' packet in a Fabric Extend carrier VLAN may trigger connected switches to respond to each other, causing high CPU utilization.
CFD-17893	A port drops a single connected device with a 'Maximum allowed MAC reached' error, disrupting mobile devices that fall back between EAP and NEAP authentication.
CFD-17926	The 'snmp-server login-success-trap' setting is not retained after a reboot, reverting to disabled even after being saved.
CFD-17927	With ECMP enabled on a Fabric Engine vIST 7830 cluster, ICMP packets to some destinations fail to leave one of the cluster members.
CFD-17951	The CLI help text for 'no ip address' describes specifying both an IP address and network mask, but the command only accepts the address.
CFD-17962	The default IPv6 route learned from a remote ISIS area intermittently disappears from the LSDB detail output (TLV 184) without a clear trigger.
CFD-17983	Unsynchronized concurrent access to the per-port silent device table may cause a switch to crash.
VOSS-35602	A false duplicate system ID conflict detected between a device and a virtual node can disable the remote ISIS instance after losing an election, preventing remote ISIS configuration.
CFD-18049	DHCP Proxy packet with source port 68 was not forwarded correctly if coming over management VLAN, causing PXE clients to fail.
CFD-18068	When a configured CA common name contains spaces, the switch sends an SCEP GetCACert request with unencoded spaces in the URL, producing a malformed request that the CA server rejects with HTTP 400.
CFD-18093, VOSS-35489	After upgrading from 9.3.x to 9.4.x, internal OSPF routes received on a non-backbone area become marked as unrestricted and fail to redistribute into ISIS, risking an outage on upgrade.

Problems Resolved in This Release	
CFD-18235	Multiple devices repeatedly lose their auto-sense connection with 'Maximum allowed MAC reached, dropping MAC' log messages.
CFD-18239	Running ' <i>show nodealias protocol-info port</i> ' from multiple SSH sessions in parallel caused the switch to crash.
CFD-18254	After upgrading a switch to 9.3.x or 9.4.x, the saved ' <i>no fa enable</i> ' setting is not applied.
VOSS-35695	The overload bit is incorrectly ignored for routes from any node with Dynamic Learned Area and overload enabled, causing a less desirable route to be preferred.
CFD-18297, CFD-18346	The OOB interface advertises two MAC addresses instead of one when it comes up, which can leave ports using MAC authentication on connected switches stuck in a held state.
CFD-18314	The help text for ' <i>show ip bgp neighbors</i> ' in the ' <i>show ip bgp ?</i> ' output displays 'Bgp' with an inconsistent capital letter instead of 'bgp'.
CFD-18358	The eBGP default-originate route is advertised with an incorrect next-hop address on some devices, causing traffic to route via an unintended next hop.
CFD-18371	An IPv6 default static route with a /127 next-hop (not supported on VOSS platforms based on RFC6164) does not come up and remains in 'not reachable' state, even though the next hop is reachable by ping.

Fixes from Previous Releases
Fabric Engine 9.4.2.0 incorporates all fixes and content from previous releases including Fabric Engine 8.10.9.0, Fabric Engine 9.0.5.1, Fabric Engine 9.1.3.0, Fabric Engine 9.2.3.0, Fabric Engine 9.3.4.0 and Fabric Engine 9.4.1.0.

OUTSTANDING ISSUES:

Please see "Fabric Engine Release Notes for version 9.4.0.0" available at <https://www.extremenetworks.com/support/release-notes> for details regarding Known Issues.

CFD-15355	Wireless clients on FA dynamic VLANs fail to get DHCP IP address when DHCP snooping is enabled. Workaround: Disable DHCP snooping globally. A fix for this issue is targeted for 9.5.0.0 release.
CFD-16869	5420 IPv4 Multicast (VRRP) in VSN ACL filter doesn't work in L3VSN. A fix for this issue is targeted for 9.5.0.0 release.
CFD-17074	Fabric Extend tunnels flap multiple times per day, correlating with ARP TTL expiration for the tunnel peer IP address. When the ARP entry for the remote tunnel endpoint expires, the tunnel temporarily goes down. Workaround: configure a static ARP. A fix for this issue is targeted for 9.5.0.0 release.
CFD-17120	When a port enters auto-sense LOOP state due to detecting both a phone LLDP and the switch's own LLDP, MAC learning and packet bridging still occur on the voice VLAN for that port, allowing a Layer 2 loop to form. A fix for this issue is targeted for 9.5.0.0 release.
CFD-17130	ECMP routing fails when the ECMP group includes both an extra VLAN on NNI path and an L2VSN path, resulting in packet loss for flows hashed onto one of the two paths.
CFD-17250	If upgrading from 8.8.1.0 to any higher release and only one of the endpoints of a 25 GbE fiber link (while the other endpoint remains at 8.8.1.0) with autonegotiation disabled on the VIM5-4YE module, the link fails to come up if FEC is set to "auto". Workaround: disable FEC or manually set it to Clause 108.
VOSS-35692	OpenAPI server fails to initialize when the bound trust point was enrolled through a Registration Authority (RA) Workaround: enroll the OpenAPI trust point without an RA or use the offline enrollment method.

KNOWN LIMITATIONS:

Please see “Fabric Engine Release Notes for version 9.4.0.0” available at <https://www.extremenetworks.com/support/release-notes> for details regarding Known Limitations.

Regular cleanup of unneeded files on USB drives is recommended to minimize possibility of USB corruption when a system is reset, shut down, or power is lost.

DOCUMENTATION CORRECTIONS:

For other known issues, please refer to the product release notes and technical documentation available at: <https://www.extremenetworks.com/support/documentation>.

GLOBAL SUPPORT

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

For the toll-free support number in your country:
www.extremenetworks.com/support/

By Email: support@extremenetworks.com

By Web: www.extremenetworks.com/support/

By Mail: Extreme Networks, Inc.
6480 Via Del Oro
San Jose, CA 95119

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

Copyright © 2026 Extreme Networks, Inc. - All Rights Reserved.

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, please see:

www.extremenetworks.com/company/legal/trademarks